Part Two

A Strategy for Action

(Intentionally Left Blank)

Chapter Five

Establishing the Partnership

Information Sharing—The Indispensable Step

Objective **Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.**

Need for Sharing Information About the Cyber Dimension

The private sector owners and operators of critical infrastructures are engaged in market-based programs offering services at competitive prices. Their risk analysis weighs the cost of physical and cyber disruption against the cost of physical and cyber security. Their willingness to invest in defenses against the cyber tools that may do harm is dependent on their experience with these disruptions and the information they have about them.

While physical security is a mature discipline, our understanding of cyber vulnerabilities and threats is incomplete. Owners and operators do not have sufficient threat and vulnerability information for informed risk management decisions. Some of the information they need may be available from the federal government, particularly from the law enforcement and intelligence communities.

As emphasized earlier, two-way sharing information is indispensable to infrastructure assurance. While infrastructure owners and operators have the fullest appreciation of vulnerabilities, they have access only to their own information or, in some cases, information pertaining to their industry or sector. Consequently, there is no comprehensive body of knowledge available for effective analysis of overall infrastructure vulnerabilities and threats. This is especially true of vulnerabilities created by increased dependence of infrastructures on one another. Current

information-sharing mechanisms perform well in matching physical threats to known vulnerabilities, and employing appropriate countermeasures. However, the same cannot be said of the emerging cyber arena.

Overcoming Reluctance

Our contacts with public and private sector stakeholders identified a need to increase the flow of information about cyber threats and vulnerabilities. Many offered a perception that private sector owners and operators share information only when they suffer substantial loss or are convinced of imminent danger to continuity of operations.

Infrastructure representatives expressed reluctance to share information about vulnerabilities because they fear it might be made public, resulting in damage to their reputations, exposing them to liability, or weakening their competitive position. Many also feared that sharing vulnerability information could invite unwanted federal regulation. The degree of reluctance varied according to infrastructure, but was present in each. The latest Computer Security Institute/FBI Computer Crime and Security Survey reinforces these observations, noting that of respondents who experienced an attack during the previous year, only 17 percent reported it to law enforcement authorities.[6]

Owners and operators told us they might have a better idea of actions they should take if the government shared more threat and vulnerability information. Likewise, government representatives told us they could better protect infrastructures if owners and operators would stop withholding information. While it is clear that government and the private sector would benefit from an improved two-way flow of information concerning threats and vulnerabilities, we caution against expecting a sudden revelation. Our classified government briefings and confidential discussions with private sector representatives produced no evidence of some missing piece of information that would make the whole picture suddenly fall into place.

Need for National Analytic Capability

Of course, sharing information isn't enough; we need the analytic tools to examine information about intrusions, crime, and vulnerabilities and *determine what is actually going on in the nation's infrastructures*. Deciding whether a set of cyber and physical events is coincidence, criminal activity, or a coordinated attack is not a trivial problem (see Figure 5). In fact, without a central information repository and analytic capability, it is virtually impossible to make such assessments until after the fact. This is of increasing concern as infrastructure operations become more reliant on information and communications—the very sector about which it is most difficult to make assessments.

[6] Computer Security Issues & Trends, Vol. III, 1997 Computer Security Institute/FBI Computer Crime and Security Survey.

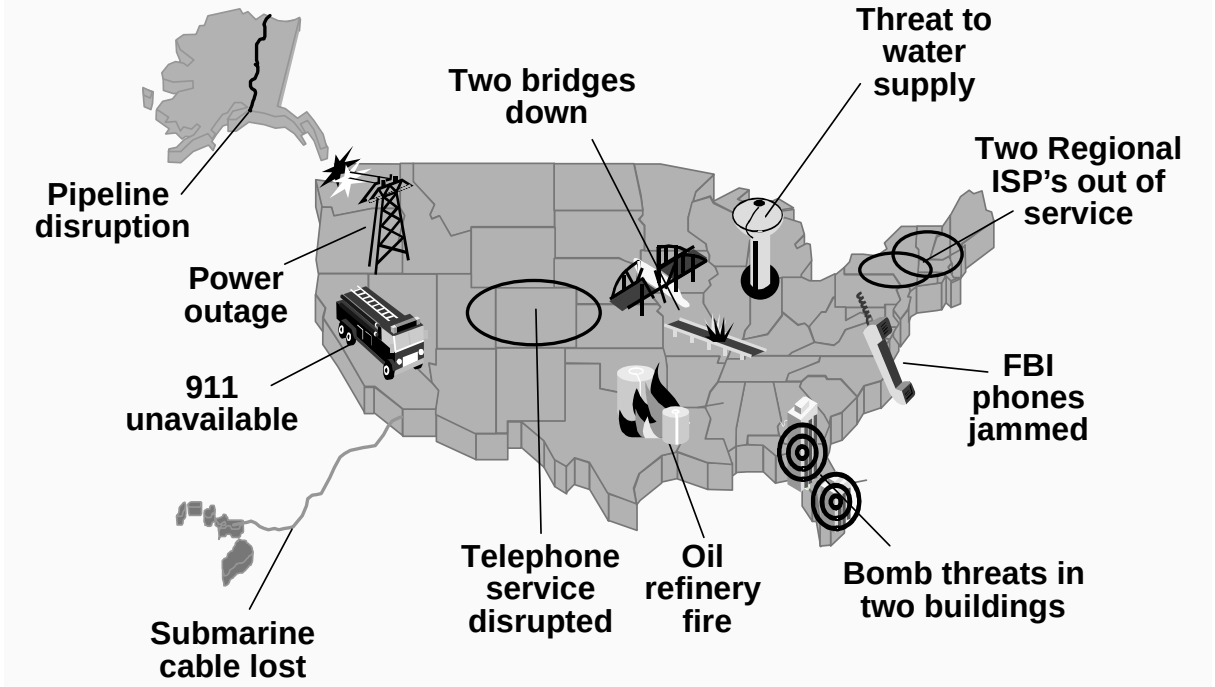

Figure 5. Coincidence or Attack?

A number of government and private organizations hold and distribute incident reports related to infrastructure protection, but comprehensive analysis of this information is limited. The need for analysis is especially critical to support decision-making about responding to attacks. There is insufficient interagency, federal-to-state and local government, or public/private correlation of data to support crisis action planning in response to a cyber terrorist incident. The need for "a cyber-threat-clearinghouse … centralized effort for comprehensive intelligence analysis of cyber issues … an industry/government information exchange for threat and vulnerability data" has been documented frequently.[7]

Existing Information Sharing Efforts

Our work did identify highly successful information sharing organizations already at work in other areas. The Centers for Disease Control and the Coordinating Sub-Group on Counter-Terrorism (CSG/CT) in the NSC are useful models for expeditious information sharing to support action planning.

[7] See, for example, The Future of US Intelligence, report by The Working Group for Intelligence Reform, 1996; NII Risk Assessment: A Nation's Information at Risk, report by the Reliability and Vulnerability Working Group, 1995; and NII: the Federal Role, report of the National Information Infrastructure Security Issues Forum, 1995. More details are contained in an internal Commission paper on Information Sharing.

We also found a great deal of information sharing already underway. Trade associations, consortia, and other groups exchange information among their members and, in some cases, directly with government. Many federal, state and local government agencies have existing relationships with infrastructure owners and operators. Within all the infrastructure sectors, at least some portions are subject to regulatory control by government agencies, and information is shared, albeit sometimes within carefully defined constraints.

Several federal agencies provide information to infrastructure owners and operators. The FBI's Awareness of National Security Issues and Response (ANSIR) program gives over 25,000 industry members information that provides threat and vulnerability insights. More narrowly focused programs are the Department of Transportation's terrorist threat notification to the civil aviation industry and the National Security Agency's INFOSEC Vulnerability Assessment Program, which provides information systems-related data to private sector partners. The Comptroller of the Currency operates another system providing advisories on information integrity and security risks to financial institutions.

Information To Be Shared

Common to most of these programs is the narrow range of information collected and shared. In almost every case, they are tightly focused on specific information with no attempt to determine whether the information might also be useful for infrastructure protection purposes. Regulatory information is not generally focused on infrastructure protection. For example, telecommunications carriers report service disruptions of 30 minutes affecting 30,000 or more customers to the Federal Communications Commission (FCC). But that reporting channel would not identify a series of smaller attacks dispersed around the country and designed to slowly weaken public confidence in the system.

Figure 6 depicts the types of information pertinent to infrastructure assurance and the likelihood that the information is reported to law enforcement. Currently, only information derived from selected threats and difficult-to-ignore, successful attacks is readily shared. This narrow range of reported types of information should be viewed as only the tip of a mountain of data whose compilation would be helpful in infrastructure

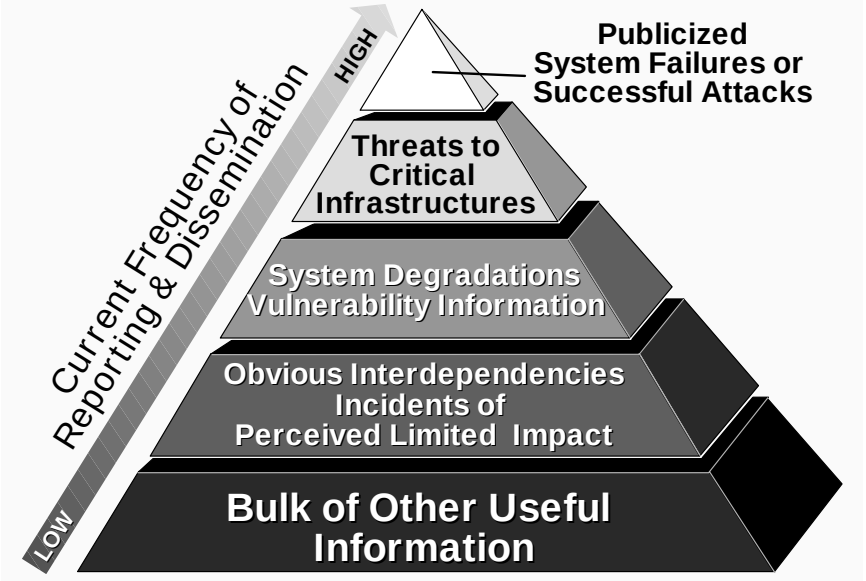

Figure 6. Scope of Useful But Unavailable Information

assurance. Included are such topics as system degradations due to physical acts or cyber-based events; vulnerabilities (hardware failure rates, operator-induced malfunctions, poor maintenance practices, or software flaws); not-so-obvious cyber or physical vulnerabilities resulting from dependence on other infrastructures; incidents of vandalism, malicious mischief, or suspicious activity; and physical or cyber anomalies. Information in government hands, such as criminal statistics and threat data, seldom is scrutinized for revelations about vulnerabilities or interdependencies. The government and infrastructure owners and operators must both push assurance-related data from the bottom towards the top of their respective agendas where it can be more readily analyzed.

Legal Impediments to Information Sharing

We envision the creation of a trusted environment that would allow the government and private sector to share sensitive information openly and voluntarily. Success will depend on the ability to protect as well as disseminate needed information. We propose altering several legal provisions that appear to inhibit protection and thus discourage participation.

Confidential Information

The Freedom of Information Act (FOIA) makes information in the possession of the federal government available to the public on request. Potential participants in an information sharing mechanism may require assurances that their sensitive information will remain confidential if shared with the federal government.

We Recommend:	The proposed Office of National Infrastructure Assurance require appropriate protection of specific private-sector information. This might require, for example, inclusion of a b(3) FOIA exemption in enabling legislation.

Trade Secrets and Proprietary Information

Private sector participants may be reluctant to share sensitive information if appropriate protection mechanisms are not incorporated.

We Recommend:	The proposed Office of National Infrastructure Assurance require appropriate protection of information containing trade secrets or other forms of proprietary information.

Classified Information

Information collected by the government to benefit a threat warning process may require protection in the form of classification.

We Recommend:	The proposed Office of National Infrastructure Assurance consider the need for classification of certain information, or certain bodies of aggregated information, and the impact that classification would have on the dissemination process.

Antitrust

Potential contributors from the private sector are reluctant to share specific threat and vulnerability information because of impediments they perceive to arise from antitrust and unfair business practice laws.

We Recommend:	The Department of Justice (DOJ) offer limited assurances to the private sector that participation in information sharing processes would not run afoul of antitrust laws and consider providing appropriate guidelines to inform participation.

Liability

Information which could prevent harm to a critical infrastructure may arise from participation in a threat and warning capability. Failure to share such information, or to act on such information shared by others, might carry liability consequences for public and private participants.

We Recommend:	The federal government undertake a detailed study of liability issues surrounding participation in an information sharing process.

National Security

Currently, many federal agencies have their own specific guidelines controlling interaction with foreign corporations or corporate entities with significant foreign ownership.

We Recommend:	The NSC study whether the federal government should standardize guidelines for sharing infrastructure assurance information with foreign corporations in light of potential national security risks and benefits.

Appropriate guidelines are needed for sharing information with foreign corporations.

We Recommend:	In the short term, the proposed Office of National Infrastructure Assurance set guidelines for the sharing of infrastructure assurance information with foreign corporations.

State Government Liability and Disclosure

Many of the legal impediments to information sharing identified at the federal level exist at the state level as well. However, diversity among state laws further complicates efforts to maximize participation in information sharing.

We Recommend:	A study group identify legal impediments to information sharing at the state level, propose solutions, and draft model legislation.

Conclusion

We believe information sharing is the critical foundation for an effective partnership to enhance our ability to protect critical infrastructures in the years ahead. Sharing information figures prominently in the additional recommendations we make and the structures we recommend for the public and private sector elsewhere in this report. How then should we build the relationship between private and public sector organizations so they can share, use, and act on information to better protect our critical infrastructures?

(Intentionally Left Blank)

Chapter Six

Building the Partnership

Owners and Operators
State and Local Governments

Objective

Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

Protecting America's infrastructures is neither an entirely public nor entirely private interest. Vulnerabilities pose risks to government, business, and citizen alike. Reducing those risks requires coordinated effort within and between the private and public sectors. The need for infrastructure protection creates a zone of shared responsibility and potential cooperation for industry and government.

Owners and operators have a responsibility to deliver reliable service. While sometimes these owners and operators are referred to as the "private sector," in truth the infrastructures include publicly-owned and operated entities such as municipal water companies, state and local highway departments, and fire, police, and emergency response agencies. Regardless of whether they are primarily accountable to shareholders or taxpayers, owners and operators must take prudent steps to reduce or eliminate their own vulnerabilities—*to protect themselves not so much against a known threat, but against the tools an unknown perpetrator could employ.*

Government has an undeniable role in accomplishing the tasks that government alone can undertake—including law enforcement at local, state and federal levels, and national intelligence, defense and diplomacy.

The Commission found a need for a new partnership between government and owners and operators to assure our critical infrastructures. And we found that the need to share information was a foundation on which we could build that partnership.

Infrastructure assurance is essentially a process of risk management. The process is generally defined to include prevention, mitigation, incident management, and recovery. The many functions associated with infrastructure assurance fit into these four categories.

In considering how these functions are accomplished today, and how they might be in the future, we identified opportunities for enhancing the effectiveness of the owner and operators through increased partnership with the federal government.

National Threats and Public-Private Partnerships

Our approach to partnership for infrastructure assurance was to examine which functions were the responsibility of each partner and the expectations associated with those functions. This led to the specific recommendations contained in this discussion about private sector, and state and local government roles.

A New and Challenging Environment

Infrastructure providers deal with known vulnerabilities and associated risks within their infrastructures. But the rapid introduction of new technologies and interconnected nature of the infrastructures present new challenges. Before interdependencies were as great as they are now, physical attacks and outages were contained. Extensive reliance on computer and telecommunications technologies makes it more difficult for owners and operators to know whether outages result from technical failure or intentional intrusion.

Further complicating the partnership is our dependence on these infrastructures for national defense, economic competitiveness, and quality of life. Realizing this certainly places the role of critical infrastructure owners and operators into new perspective. While they must still respond to normal business pressures—the bottom line, shareholder concerns, and their customers—they must also acknowledge that the government has an increasing interest in infrastructure providers. The critical role of many public utilities exemplifies this situation where health, safety and other public concerns are so dependent on the infrastructure that government interest is unquestioned. Today, the interconnected nature of the infrastructures, the potential for local disruptions to cascade into other infrastructures, and the dependence of national security on those same infrastructures present a clear need to think in new ways.

These facts alone emphasize the need for infrastructure owners and operators and government at all levels to find new ways of working together. These new partnerships must be designed to

foster mutual trust and facilitate sharing of the types of information that each partner needs to assure the uninterrupted flow of essential goods and services.

Expectations of Owners and Operators[8]

Owners and operators are the primary players in infrastructure assurance. For all the expected business and operational reasons, they protect their critical systems and facilities based on a perceived set of risks. Better information on emerging threats and vulnerabilities, particularly those stemming from unrecognized or little understood interdependencies, will assist managers in making decisions about investment in security processes, thus improving assurance not only for their own company's operations, but for operation of the infrastructure overall.

The Commission believes it is the responsibility of owners and operators to:

1) Provide and manage facilities delivering services to customers efficiently and effectively.
2) Meet customer expectations for quality and reliability of service.
3) Maintain an effective risk management process adequate to:
    - identify vulnerabilities and potential threats that might affect continuity of service;
    - prevent and mitigate as many credible threats as economically feasible; and
    - maintain emergency response capability to quickly restore service and eventually reconstitute the infrastructure in the event of service interruptions.
4) Give special consideration to the vulnerabilities currently in many information systems.
5) Cooperate within their industry to identify best practices for improving service reliability and security.
6) Report possible criminal activities to law enforcement agencies and cooperate with investigations.
7) Establish a relationship with intelligence and law enforcement to assure that information about warnings and threats is communicated in a timely way and that the industry experience with incidents is available as an input to threat analysis.

[8] As previously noted, the term "infrastructure owners and operators" includes public agencies or corporations as well as companies and activities in the private sector.

Risk Assessment Best Practices

Conduct a security training program for all employees according to their job responsibilities and access authorizations, integrating this program with existing physical security aspects.

Authenticate the identity of all users of the system, determine the uses of the system for which they are authorized, and restrict access to only the authorized functions and data.

Isolate critical operational control systems from all public and most internal networks, or provide adequate firewalls.

Provide adequate procedural and technical controls to assure data integrity, to detect instances of unauthorized change or deletion, and to recover when necessary.

Authenticate and log the origin of all commands to change the operating conditions of the controlled infrastructure.

Create a CERT, or similar response capability, with the equipment and training needed to investigate suspected intrusions, isolate and recover damaged systems, and restore service to customers.

Provide adequate back-up and recovery capability for the programs and data of any information system that is necessary for normal operations and customer service. To better assure the availability of key control systems, information systems and data, consider redundancy, geographic separation of primary and back-up systems, alternative methods, effective use of encryption, and other relevant security options.

Conduct regular assessments of the vulnerability of information systems using the technical expertise of the National Security Agency (NSA) and others as appropriate to assure that new techniques for attacking systems can be contained by the protective measures currently installed.

Compiled by the President's Commission on Critical Infrastructure Protection

Industry Suppliers

Usually the owners and operators are not the suppliers of the computer hardware and software they use to manage their operations. For significant improvements to be made in the security and integrity of these information systems, suppliers must be involved.

The computing systems industry is highly competitive and normally very responsive to customer needs; however, experience suggests that users may not understand the new vulnerabilities well enough to demand products offering better security. There is recent evidence that major suppliers are giving security and integrity more attention than in the past. We expect this trend to accelerate as owners, operators, and industry associations study their vulnerabilities and demand improved products.

Vulnerabilities Assessments

The more owners and operators understand about their vulnerabilities (see Figure 7), the better able they are to make effective decisions about protecting their operations. A step toward increasing private sector awareness can be taken by increasing federal government participation in the vulnerability assessments conducted by owners and operators.

We Recommend:	The NSA, the Department of Energy (DOE) and DoD: • continue to perform vulnerability assessments for critical infrastructure owners and operators. • provide vulnerability assessment training to private sector service providers on a cost-reimbursable basis, e.g. sharing knowledge and expertise of key government centers of excellence.

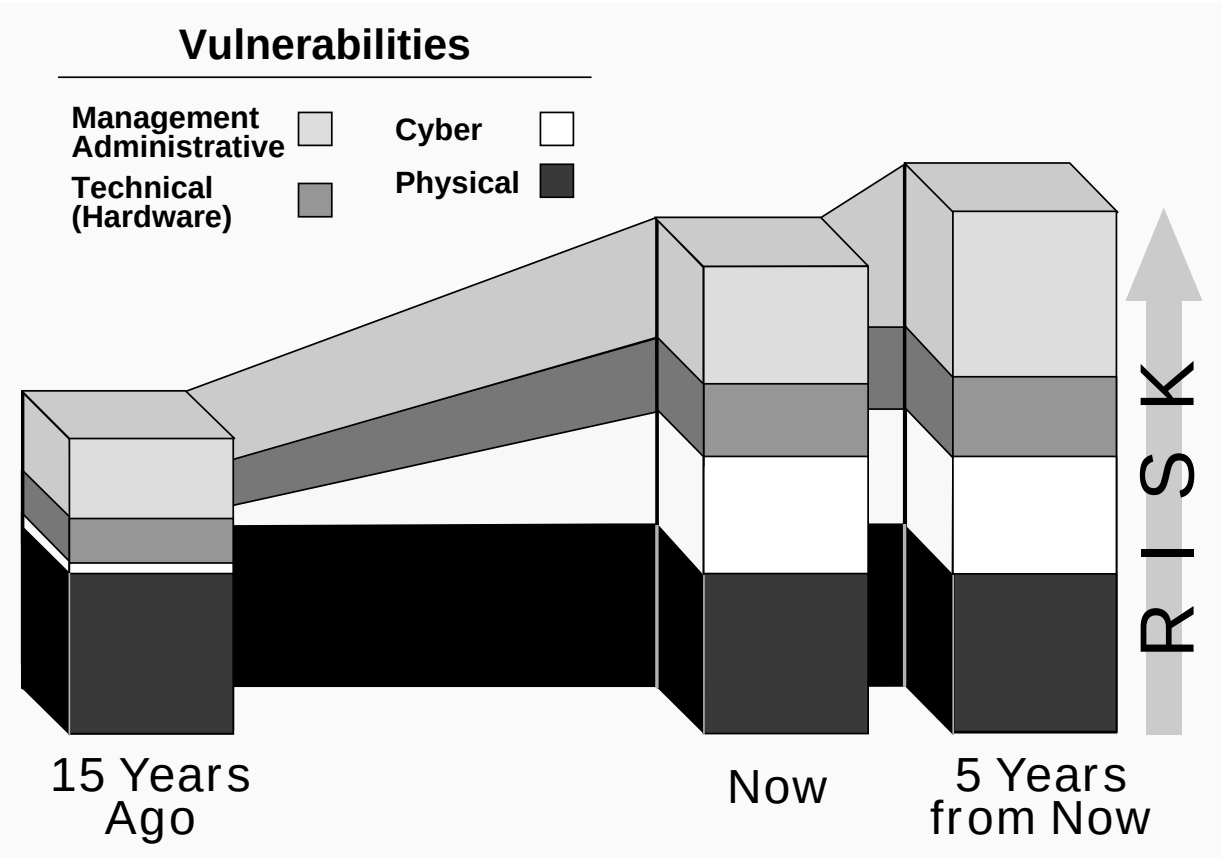

Figure 7. Vulnerabilities Profile

Publicize & Support Application Of Risk Assessment Methodologies

We Recommend:	The proposed Office of National Infrastructure Assurance and National Infrastructure Assurance Council encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems. This will enable more informed risk management decisions in the face of rapid, pervasive change.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage the insurance industry to develop its risk methodologies for application to the critical infrastructure industries.

Sensitive Information

In Chapter 5, we described the need to overcome the concern of owners and operators that information they provide to government might not be protected. As the importance of the infrastructures to every aspect of national strength is understood, information that may be useful to an enemy in designing an attack on those infrastructures takes on a new importance.

One example of concern in this area is found in requirements for publication of sensitive information about critical components or the functioning of infrastructures. This information has the potential to serve as a "road map" for a potential infrastructure attack; therefore, its publication may lead to the exploitation of vulnerabilities.

We Recommend:	The President issue an Executive Order requiring that federal agencies accomplish the following before publishing or requiring the publication of information about critical components or functioning of infrastructures. • bring together the relevant stakeholders to discuss the implications of the requirement. • identify the purpose for publishing the information and ensure that the information is published in a format that minimizes the likelihood it will be used in ways that are incompatible with infrastructure assurance. • certify that the positive and negative effects on infrastructure assurance have been fully explored, including that the potential benefits of publication outweigh any identified risks.

Protection of Infrastructure Vulnerability Information

We now must question whether information regarding vulnerabilities—in the aggregate at least—shouldn't be protected in some fashion.

We Recommend:	The US Security Policy Board be tasked to provide a recommendation to the President on criteria for and means of protecting otherwise unclassified private sector information on threats and vulnerabilities to critical infrastructures.

Publication of Infrastructure Assurance Data

The publication of infrastructure assurance-related comparative data within an industry may positively influence performance by motivating increased attention to information security, as well as reliability, without resorting to regulation. This information may prove useful to consumers in light of increased competition and choice between providers of critical infrastructure services. We found such reports of great use in some infrastructures. In electric power, for example, the NERC publishes each month on its WWW site a Performance Honor Roll of companies achieving 95 percent or better reliability in the previous 12 months.

We Recommend:	The Administration direct the FCC's Network Reliability and Interoperability Council to initiate a feasibility study of publishing comparative infrastructure assurance-related data for the telecommunications industry. The study should focus on whether publication is likely to achieve infrastructure assurance objectives, the types of data to collect and publish, whether current data collection efforts are sufficient, and other possible impacts of publication. Similar studies should follow for other infrastructures.

Security Standards

The Commission considers the development of standards to be the responsibility of the infrastructure operators themselves. In our research, we were advised of an initiative of the NERC to apply mandatory reliability standards (which include security) to its members. Currently, the Federal Energy Regulatory Commission (FERC) is dealing with this issue for the whole electric power industry. The activities of these two organizations are headed in directions the Commission applauds and recommends to other infrastructure sectors.

However, we do believe that government should encourage and assist public and private sector standard-setting bodies to broaden their areas of responsibility regarding reliability to include security assurance.

We Recommend:	The National Institute of Standards and Technology (NIST) and NSA work with the proposed Office of National Infrastructure Assurance to offer their expertise and encourage owners and operators of the critical infrastructures to develop and adopt security-related standards. Relevant federal and state regulatory agencies, industry associations and standards groups, and law enforcement and intelligence agencies should also participate in the process of identifying and developing standards.[9] These standards should address not only the technology itself, but also ancillary topics such as tools, policies, procedures, and practices.

Building the Partnership
State and Local Government

State and local governments are integral to the success of the partnership we propose for infrastructure assurance. State and local governments' infrastructure roles cut across the public-private boundaries. They operate infrastructures—certainly emergency services, but also water systems and a host of other vital services. They are also the regulators of many of the infrastructures—particularly those considered to be public utilities. And finally, they are users of the infrastructures—just as dependent on information and communications, energy, and transportation as the federal government.

We met dozens of local officials and held public meetings on infrastructures around the nation. State and local officials consistently expressed their need for federal assistance in key areas relating to infrastructure protection.

High on their agenda is raising public awareness on infrastructure matters, particularly in protecting information networks. They need assistance from the federal government in maintaining competent trained firefighters, policemen, and paramedics prepared to handle infrastructure disasters and threats from chemical, biological, and radiological materials. They need solutions

[9] Standard-setting groups include the American National Standards Institute, the Institute of Electrical and Electronic Engineers, and the National Computer Security Association.

in addressing the crowded spectrum of radio frequencies that emergency services must use to communicate. And they need a forum to share information on infrastructure issues.

Sharing Information

Organizations representing state and local interests have existing relationships with federal government officials. By working through such organizations, we can effectively share information on protecting our critical infrastructures.

We Recommend:	The proposed Office of National Infrastructure Assurance lead the way in making information about infrastructure assurance available to state and local governments through existing organizations such as the National Governors' Association.

Equipping and Training First Responders

The Commission's research found emergency services ill-prepared to deal with chemical and biological attacks. Few "first responders"—firefighters, police, and paramedics—are adequately trained to treat attack victims or equipped with protective gear or supplied with medical treatments, such as atropine.

Legislation initially sponsored by Senators Nunn (D-GA), Lugar (R-IN), and Domenici (R-NM) focused federal resources on providing training, equipment, and information to local first responders. State and local police, fire, and medical officials are requesting an expanded effort in this area, and the Commission agrees that these efforts should be intensified and made more widely available.

We Recommend:	DoD, the Department of Health and Human Services (HHS), and the FBI provide local first responders additional training and equipment for improving the detection, identification and management of chemical, biological, and radiological incidents. Domestic preparedness funding (Nunn-Lugar-Domenici) for these activities should be doubled in FY99.

Spectrum Allocation

Police, firefighters, paramedics, and repair crews must be able to communicate clearly during emergencies. The radio frequencies used for dispatching and communication are congested—making it difficult to use the spectrum effectively.

The FCC has been auctioning segments of the electromagnetic spectrum. As demand rises for commercial bandwidth, spectrum becomes increasingly scarce, placing non-revenue generating public sector users, such as federal, state and local emergency services, under increasing pressure to relinquish relatively under-used portions of their bandwidth allocations.

Addressing this issue, the National Telecommunications Information Administration (NTIA) and the FCC-sponsored Public Service Wireless Advisory Committee (PSWAC) issued a joint recommendation, which the Commission endorses, that the FCC designate inviolate spectrum segments for emergency services—removing them from future auction consideration.

Should circumstances require spectrum reallocation, however, the FCC should ensure compensation of state and local emergency service providers for the costs of replacement equipment, training, and transmission capabilities.

We Recommend:	Expanding NTIA's mission to include representing the interests of state and local governments in addressing access to and use of the electromagnetic spectrum. This advocacy should include efforts to ensure that current needs of these governments are identified and appropriately balanced with commercial and federal sector needs, that interoperability requirements among emergency services—in locales as well as regionally and nationally—are considered, and that adoption of new services and technologies is both facilitated and coordinated across all government levels.

We Recommend:	The FCC and NTIA expeditiously adopt the PSWAC recommendations. In particular, the FCC should: • allocate an additional 25 MHz of unencumbered spectrum for public safety. • provide 2.5 MHz in the VHF and UHF bands for interoperability among emergency service providers. • plan for allocation of an additional 70 MHz for new technology applications in law enforcement and emergency services. • immediately factor other detailed recommendations of the PSWAC into the spectrum allocation planning process.

These measures will assist state and local governments in meeting their critical infrastructure protection responsibilities, but they are only a first step. We fully recognize that the challenges facing state and local governments go well beyond what can be addressed by the application of such limited means.

Conclusion

In the interconnected, cyber-oriented world of today, the responsibility for infrastructure assurance cannot be divided along traditional lines between government and the private sector or allocated among levels of government. The need to forge a partnership between all players—to achieve joint, integrated, and complementary action—is more acute than ever. With a better understanding of the expectations and roles of the owners and operators, and of state and local governments, comes an appreciation for their increasingly "front line" mission in defending our infrastructures. The federal government should structure itself for its own mission of infrastructure assurance—a mission that now includes facilitating and supporting the efforts of critical infrastructure owners and operators.

(Intentionally Left Blank)

Chapter Seven

Structuring the Partnership

Objective

Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning and programs.

Early in the Commission's deliberations, we recognized the federal government was still organized along Cold War lines. The structures in place had proven very effective at focusing federal attention and resources on physical threats posed by military, terrorist, or criminal entities. Likewise, the relationships between government agencies and infrastructure operators were appropriate to the environment. Except for down-sizing, the structure of the federal government had not changed significantly since the Cold War, and its relationships with infrastructure owners and operators—though less regulatory in nature—had not changed markedly (see Figure 8).

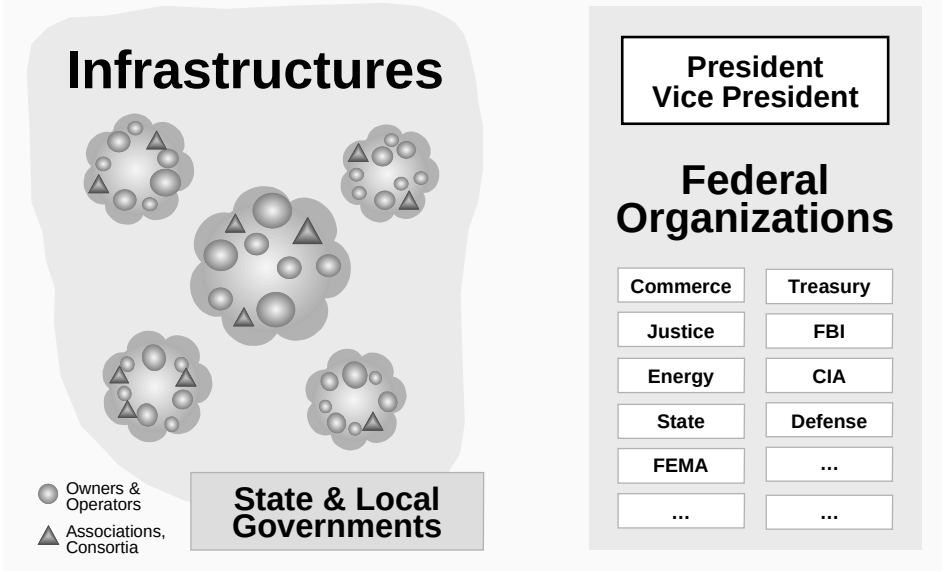

Figure 8. Infrastructure Assurance Today

But the federal government today must address the emerging threats to our infrastructures, the new geography discussed earlier in this report, and the requirements of the Information Age. How the government organizes itself is a key factor in the partnership with infrastructure owners and operators that is fundamental to meeting the

challenges of the threats we share. Without recommendations that set out clear national organizational structures, the chance for developing a government and industry partnership could elude our grasp.

To address these organizational issues, we examined the functions or actions instrumental to achieving infrastructure assurance and protection at the national level. In each of the five functional areas, the need for partnership and dynamic interaction between the government and infrastructure owners and operators is apparent, as indicated below.

Policy Formulation—The federal government can best assess emerging threats, and the owners and operators can best assess their vulnerabilities. Together they should assess the national risk and determine assurance objectives, strategies, and policy.

Prevention and Mitigation—Owners and operators will have to examine the vulnerabilities of their own systems and networks and put in place the protective measures and practices needed to achieve target levels of assurance. The government can and should support these efforts through R&D, awareness and education, threat assessments, initiatives to facilitate private sector adoption of best practices, and , possibly, through direct financial assistance.

Information Sharing and Analysis—The key products of this functional area are answers to two questions: (1) What unusual is happening among our infrastructures, and (2) what unusual is happening among our adversaries? Owners and operators should take the lead for the former; the federal government (law enforcement and intelligence) for the latter. Analyzing the information provided and synthesizing it into advisories and warnings should be a shared responsibility.

Counteraction (incident management)—The objective of this functional area will be to deter an attack on our critical infrastructures, and, should deterrence fail, to cause the attacker to cease and desist. This area is clearly a federal responsibility, primarily of the law enforcement and defense communities, but there are many important ways in which the owners and operators can and should assist.

Response, Restoration, and Reconstitution (consequence management)—Responding to the basic needs of the populace following a disaster is a responsibility of the states, supported by the federal government. Restoring and reconstituting infrastructures is the responsibility of the owners and operators, supported by their sector. A major restoration and reconstitution effort would require coordinated public and private sector actions.

As we sought to identify what sorts of national structures would best accomplish these functions, we applied the same principles used to guide all of our deliberations.[10]

[10] These guiding principles are discussed in Chapter 4.

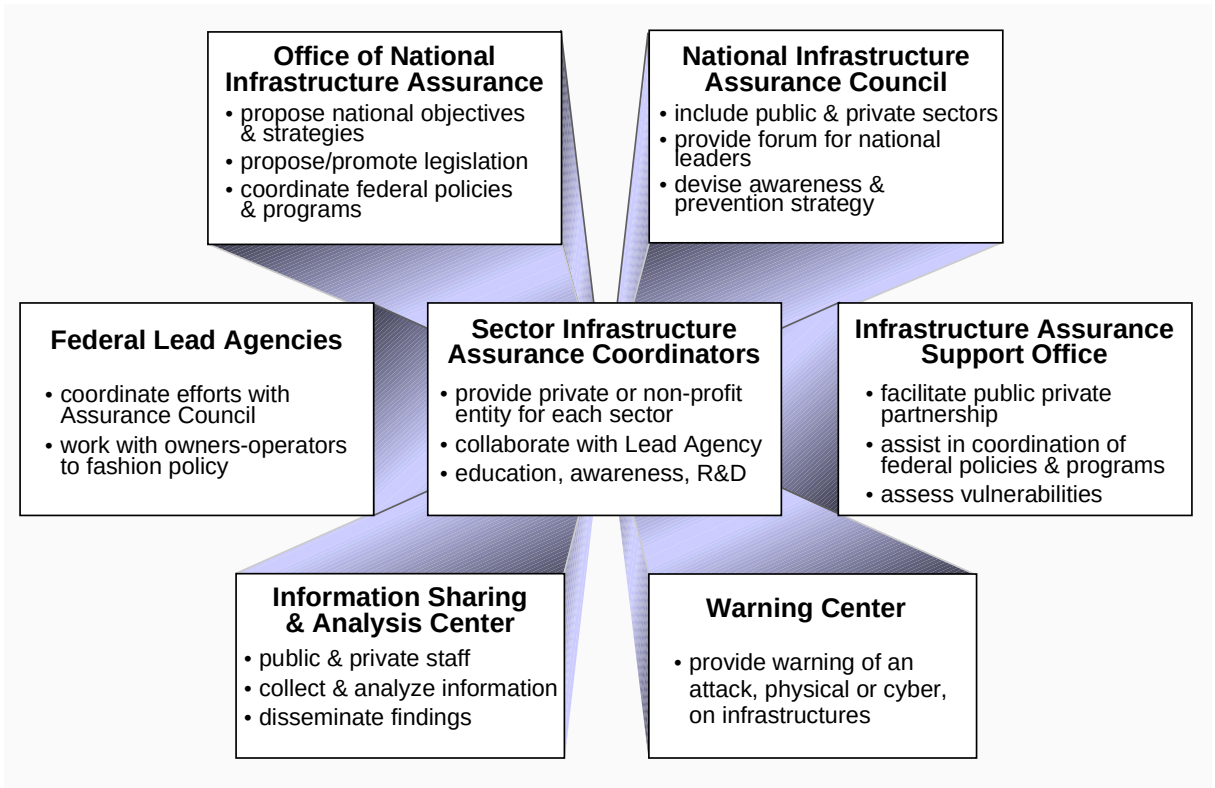

Figure 9. Proposed Roles and Responsibilities

Proposed National Structure for Infrastructure Assurance

The Commission proposes a set of structures and processes within the public and private sectors to facilitate infrastructure assurance functions and complement existing law enforcement, regulatory, and other channels of communication between and among critical infrastructure providers and the government. These new structures and processes will provide trusted and protected channels for sharing public and private infrastructure assurance information, and a means for focusing, enhancing, and generating additional infrastructure assurance efforts throughout the federal government and private sector.

Essentially, we envision the proposed infrastructure assurance structure for the United States as consisting of seven elements (see Figure 9). Each is discussed in detail below.

- An ***Office of National Infrastructure Assurance*** in the White House to serve as the focal point for infrastructure assurance.

- A ***National Infrastructure Assurance Council*** of prominent infrastructure corporate leaders, representatives of state and local government, and Cabinet officers to address infrastructure assurance policy issues and make appropriate recommendations to the President.

- An ***Infrastructure Assurance Support Office*** to provide functional support and management of the federal organizations involved in infrastructure assurance, as well as providing direct assistance to the public and private sector partnership effort.

- A federal ***Lead Agency*** for each sector to take the initiative in bringing together the owners and operators to create a means for sharing information that is acceptable to all.

- A ***Sector Infrastructure Assurance Coordinator*** for each infrastructure to function as a "clearing house," organizing information sharing activities, protecting the information provided by each participant, and acting as a channel for information to, and from, the government.

- An ***Information Sharing and Analysis Center*** consisting of government and industry representatives working together to receive information from all sources, analyze it to draw conclusions about what is happening within the infrastructures, and appropriately inform government and private sector users.

- A ***Warning Center*** designed to provide operational warning of a physical or cyber attack on the infrastructures.

No office, organization, or individual within the federal government has overall responsibility for infrastructure protection or policy. This is not surprising as there was little need for a national focal point when infrastructures were largely independent, discrete, insulated by geography and protected by military defenses. Today, however, the interdependent, interconnected nature of the infrastructures, and their exposure to cyber and other threats, creates a real need for a single point of focus. To support this, a federal framework needs to be created, working in conjunction with state and local governments and the private sector, to implement a national policy on infrastructure protection.

Our first recommendation for structuring the partnership between government and industry addresses this need for national focus by creating an Office of National Infrastructure Assurance.

Office of National Infrastructure Assurance ("National Office")

We Recommend:	The President establish a Office of National Infrastructure Assurance within the NSC staff, Executive Office of the President, directed by a Special Assistant to the President. The primary functions of the National Office would be government-wide policy formulation, oversight of government activities in infrastructure assurance and cyber security issues, and coordination of cyber support to existing and planned decision-making processes in the law enforcement, national security, counterterrorism, and intelligence areas.

The specific duties and functions of the National Office would include:

1) Oversee and facilitate infrastructure assurance policy formulation to include assessing the national risk, integrating public and private sector perspectives, proposing national objectives, developing implementation strategies, proposing and promoting new legislation, assessing the need for new regulations, providing oversight and functional management of infrastructure assurance budgets, and issuing national policy.

2) Encourage and support private sector prevention and mitigation activities including coordinating education programs, legislative and regulatory support to the establishment of standards, certifications and best practices, developing assessment instruments, and developing research requirements.

3) Oversee the creation, management, and operations of the other structures recommended in this report. The National Office would have special responsibility for oversight of the Information Sharing and Analysis Center, recommended below.

4) Review plans, sponsor appropriate training, and assess operational readiness. In the event the operational control of response to an attack on US infrastructures is elevated to the NSC, the staff of the National Office would serve as the secretariat to the NSC entity managing the crisis.

While this office would not have any operational responsibility for responding to an attack, we envision it as the channel through which federal cyber expertise and resources would be identified and made available to the decision-makers, planners, and the designated lead agency responding to an attack.

We envision this as a very small office, consistent with White House staffing standards. About ten senior personnel should be detailed from pertinent government agencies.

National Infrastructure Assurance Council ("Council")

We Recommend:	The President appoint a high-level council comprised of Chief Executive Officers (CEOs) from throughout the critical infrastructures, senior government officials (Cabinet rank), and representatives of state and local government. The Council would meet regularly to provide a forum for high-level discussion of proposed policies and directions for the nation in this critical area, to encourage and advocate partnership in infrastructure protection, and to make appropriate recommendations to the President.

The Council should provide policy advice to the President. It should meet no less than twice annually, and create whatever sub-structure it needs. A standing executive committee consisting of the Chair, selected Council members, and the Director of the National Office should meet often to manage the Council's work.

Staff support would be provided by the National Infrastructure Support Office. Members of the Council should be permitted to contribute staff and program support from their organizations (both public and private) to assist the Council in its work. Specific functions and duties of the Council should include:

1) Serve as the forum for national debate on infrastructure assurance issues.

2) Promote national objectives and strategies, facilitating discussion among the major stakeholders and government.

3) Review proposals from industry or government for mandatory standards, certifications, and best practices.

4) Provide leadership, advocacy, and support for the education and awareness efforts required to enhance national understanding and support for infrastructure assurance activities. Specifically, the Council should consider advocating, supporting, and encouraging adoption and use of "business" risk assessment tools and methodology.

5) Assist in setting directions for R&D program.

While the National Office and the Council provide avenues for the high level communication needed to develop a partnership in support of infrastructure assurance, the key to success in this arena rests with the existing federal agencies and the infrastructure sectors themselves.

Infrastructure Assurance Support Office ("Support Office")

We Recommend:	The President create a functional office to support infrastructure assurance activities throughout the federal government and the private sector.

The National Office would direct the activities of the Support Office, but it would be located in, and supported by the US Department of Commerce (DOC). The Support Office should be a joint coalition organization, bringing together appropriate national security and non-national security components. Staffing for the new office should reflect this mix among the required 20-30 professional, technical, and support staff including full-time employees, reimbursable details from other federal agencies, and private sector staff obtained under the Intergovernmental Personnel Act or by other means.

Its primary mission would be to support the National Office and the Council. Principal functions for the Support Office would include:

1) Support policy formulation by managing the national risk assessment, providing staff support to the Council and its subcommittees, tracking legislative and regulatory agendas, providing technical assistance to the Sector Infrastructure Assurance Coordinators, consolidating budget requests, drafting the budget proposal, establishing a system for tracking accomplishments, drafting the annual policy, and managing production and distribution.

2) Support prevention and mitigation by assisting the Council and the sectors in consolidating training requirements and developing new programs; by assessing current standards, certifications and best practices; by developing vulnerability assessment instruments (in consultation with the Sector Infrastructure Assurance Coordinators and selected owner and operators) and providing training in their use; and by coordinating the research program.

3) Assist the proposed National Office in the management of the Information Sharing and Analysis Center.

4) Assist the NSC in the preparation of stand-by plans and authorities in coordination with the relevant agencies and private sector entities; and provide technical support to the FBI and Federal Emergency Management Agency (FEMA) for development of policy and plans to manage incidents and consequences.

Federal Lead Agencies ("Lead Agencies")

We Recommend:	The President designate specific federal agencies to take the initiative in bringing together the owners and operators of various infrastructure sectors to create a means for sharing information that is acceptable to all participants. Lead Agencies will not replace the existing relationships, or assume any of the responsibilities of the law enforcement, regulatory or other special function agencies. They will work with sector owners and operators to identify and implement a method of sharing and protecting information.

Many federal and state agencies have interests and responsibilities in the infrastructure sectors. Additionally, each sector is comprised of diverse companies, associations and consortia which may challenge efforts to share information. Assigning leadership responsibility to the highest levels within identified federal agencies creates an opportunity to advocate and generate common purpose among the infrastructure leadership. We anticipate that Lead Agencies will coordinate with the Office of National Infrastructure Assurance to obtain the authorities needed to accomplish the following functions.

1) Establish and maintain channels of communication with all private and public entities having an infrastructure assurance interest in the sector.

2) Facilitate the selection of a Sector Infrastructure Assurance Coordinator (described below).

3) Assist the Sector Coordinator in establishing and operating an effective information sharing program.

4) Provide input to national infrastructure assurance objectives and strategies.

5) Draft new legislation and regulations, as required, and propose the use of federal incentives to facilitate private investment in assurance programs if appropriate.

6) Promote infrastructure assurance education and training, to include advocating use of best practices, within the sector.

7) Assist in developing plans for prevention (long-term reduction of vulnerabilities and short-term defensive actions), mitigation, restoration, and reconstitution.

8) Coordinate, in support of the Federal Response Plan (FRP), as amended, management of the consequences of a successful infrastructure attack and prepare for various contingent attacks through participation in training and exercise programs.

While assigning Lead Agency responsibilities for all critical infrastructures may be novel in some infrastructure areas, in others such a relationship already exists. Clearly, the Departments of Transportation and Energy already perform many of the responsibilities we outline for Lead Agencies. In other infrastructure sectors, telecommunications and information, for example, both DoD and DOC have significant interest and existing relationships in these infrastructure sectors. After much debate, we arrived at a proposal for assigning Lead Agency responsibilities for each infrastructure sector, shown in Table 2.

Table 2. Proposed Lead Agencies

Infrastructures from EO 13010	Commission's Infrastructure Sector	Proposed Lead
Telecommunications	Information & Communications	Joint Department of Defense & Department of Commerce
Electric Power	Electric Energy	Department of Energy
Gas & Oil	Gas/Oil Production & Storage	Department of Energy
Banking & Finance	Banking & Finance	Department of the Treasury
Transportation	All Sub-sectors	Department of Transportation
Water	Water Supply	Environmental Protection Agency
Emergency Services	Emergency Services	Federal Emergency Management Agency
Continuity of Government	Government Services	Office of National Infrastructure Assurance

Perhaps the most challenging responsibility of the proposed Lead Agencies will be facilitating the selection, by the owners and operators, of Sector Infrastructure Assurance Coordinators.

Sector Infrastructure Assurance Coordinators ("Sector Coordinators")

We Recommend:	Each infrastructure sector select or create an entity to facilitate sharing information among providers and with government. These Sector Coordinators will lead the sector in determining, collectively, how best to share the type of information needed for infrastructure protection by the federal government and owners and operators they represent.

Each sector will determine the particular mechanism best able to meet its needs. In some, an association or set of associations may best serve the industry and accomplish the role outlined here. Totally private and voluntary organizations may be selected by some, while others may find an existing regulatory agency more useful in the lead role.

Lead Agencies (described above) will work with infrastructure owners and operators and other government agencies that have industry-specific missions to establish these communication, coordination, and sharing mechanisms. Some sectors already have the kind of industry-wide organization needed. One example of such a partnership is the NERC.

Where a sector has such diverse interests that it cannot settle on a single Sector Coordinator, owners and operators and the Lead Agency may explore innovative solutions, such as a "virtual coordinator" based on existing networked resources.

The functions envisioned for the Sector Coordinators include:

1) Provide the sector with a means to accumulate information, disguise identity of providers, transmit information to the public-private Information Sharing and Analysis Center (described below), receive information from the Center, and disseminate it to the sector's owners and operators.
2) Serve as the focal point within the sector for risk assessment activities; and represent the owners and operators in discussions with other entities of the infrastructure assurance structures as needed.
3) Serve as the clearing house and hub for information sharing within the sector, assist in the analysis of anomalous events, and prepare statistical summaries.

Sector Coordinators will provide the central conduit for the information needed to develop an accurate understanding of what is going on throughout the nation's infrastructures. That is the purpose of the most innovative structure we recommend, a public-private analytic organization.

Information Sharing and Analysis Center ("Center")

We Recommend:	The President propose, and Congress charter, a new organization staffed by federal government employees and infrastructure owner-operator representatives to provide the analyses needed for infrastructure protection. The Center would receive information from all relevant sources, analyze it to determine what is actually happening in the infrastructures, and appropriately inform government and private sector users. Legislative changes will be required to implement this recommendation.

To be effective, the Center must have benefit of the legal initiatives discussed in Chapter 10, including some means to protect sensitive private sector information shared with the government and authority to negotiate non-disclosure agreements with the private sector. It should have direct channels to all interested government agencies to facilitate the flow of information.

Initially, the Center would focus on gathering strategic information about infrastructure threats, vulnerabilities, practices, and resources that will enable effective analyses to better understand the cyber dimension associated with infrastructures. The analysis produced will also allow more effective planning and decision-making about investments required within and outside the government. This information would include technical information of interest to owners and operators needing to better protect their systems from cyber attacks and threat-specific information developed by the government and provided through the Center to the infrastructure owners and operators. The Center would be expected to gather and maintain information about available assurance, protection, and defense resources within both public and private sectors for protection from cyber attack. Additionally, this Center would provide a one-stop/one-call capability for infrastructure assurance with special emphasis on the cyber dimension. When infrastructure owners and operators perceive problems within their information systems, they could call the Center to receive immediate information about available assistance.

The Center will, based on its analysis, issue bulletins, advisories, and other communications that will enable the infrastructure owners and operators to enhance their own levels of protection. It will also provide analysis to the FBI for dissemination to government agencies as required, and to the National Office and Support Office to be included in the policy, planning, R&D, budgeting, and other processes.

The responsibilities envisioned for this Center are:

1) Review reports of unusual occurrences from the owners and operators and the government, and prepare advisories for open release to the infrastructure providers through their Sector Coordinators and the government concerning vulnerabilities, failures, and system deficiencies.

2) Receive intelligence and law enforcement information concerning the development of potentially damaging tools and threats, and prepare advisories.

3) Enable the receipt and validation of anonymous data.

4) Provide technical assistance on a 24-hour basis.

5) Establish an extensive analytical data base accessible by the owners and operators and the government.

The proposed Center should eventually be staffed with between 20 and 40 personnel, about half of whom should be representatives from the infrastructures. Specific cost-sharing details can be negotiated, but to facilitate the speedy implementation of this recommendation, the government should be prepared to deploy the entire "start-up" cadre. The location of this Information Sharing and Analysis Center should be high on the agenda for decision by the Office of National Infrastructure Assurance. We believe an interagency group should investigate creative siting alternatives, especially locating it in the private sector. A number of excellent possibilities are available, among them co-locating with the Carnegie-Mellon University's CERT, another CERT, or a Federally Funded Research and Development Center, or contracting to a private entity (or university).

A significant aspect of the Center would be a government-only cell connected to the FBI's Office of Computer Investigations and Infrastructure Protection (OCIIP), which would serve as the preliminary national warning center for infrastructure attacks and provide the Center with law enforcement, intelligence, and other information needed to ensure the highest quality analysis possible.[11]

Information sharing and analysis will go far toward enabling the infrastructures to better protect themselves and ensuring the government has a more effective picture about what is happening throughout the infrastructures. This will allow us to understand whether diverse events—physical and cyber—are actually coincidental or related actions in an attack on different pieces of our infrastructures.

A Step Toward A National Cyber Warning Capability

We believe the eventual goal in this area is an indications and warning capability that provides immediate, real-time detection of an attempted cyber attack on critical infrastructures. The model for what we have in mind is the air defense and missile warning system. This is a defense system consisting of a monitoring or sensor capability, an analytic capability, and an alerting capability.

[11] In July 1996, the Director of the FBI established the Computer Investigations and Infrastructure Threat Assessment Center (CITAC) as a single point of coordination for all criminal, counterintelligence and counterterrorism computer intrusion matters and cases involving threats to critical infrastructures. In August 1997, the Director upgraded the status of this coordination function by creating the OCIIP.

Until we are able to field a real-time warning capability, we will need to rely on the proposed Information Sharing and Analysis Center described above and on existing government warning or watch centers. The FBI's newly-established OCIIP currently has the most potential for this effort and should assume the Warning Center responsibilities. In fact, the FBI has recently established and begun to staff a multi-agency Watch and Threat Analysis Unit within OCIIP. This unit's goal is to use existing criminal, counterintelligence, and counterterrrorism authorities to meld information from government sources and cooperating private sector entities to detect cyber threats to critical infrastructures. It will act on that information to provide tactical warning of immediate consequence. OCIIP will use existing mechanisms to issue cyber threat alerts in the same way the FBI now issues terrorist alerts. As new capabilities come on line in the Information Sharing and Analysis Center and with Sector Infrastructure Assurance Coordinators, we expect they will enhance the FBI's alerting mechanisms.

To integrate the capabilities being developed in OCIIP with those proposed elsewhere in this report, the Commission suggests that the OCIIP's function be expanded to include:

1) Operating near real-time secure communications with the proposed Information Sharing and Analysis Center on a 24-hour basis, in addition to the connectivity already being established by the Watch and Threat Analysis Unit with other government watch offices.

2) Integrating anomalous infrastructure events with intelligence and law enforcement information for the purpose of developing indicators that the nation may be "under attack." When such an indication is forthcoming, the FBI would make appropriate notifications and issue warnings, and would alert the Information Sharing and Analysis Center to prepare and disseminate bulletins and threat advisories to infrastructure stakeholders.

We consider development of a warning capability to be of fundamental importance to the future security of our nation. We urge the Director of the FBI to continue to enhance the capabilities of the OCIIP and we reinforce the FBI's requests for the funding needed to establish and maintain capabilities in the cyber arena—beyond those needed for the investigation of criminal, counterintelligence and counterterrorism cases—to include the analytic capacity and the R&D efforts related to threat detection that will enable real warning in the years ahead.

Tables 3 through 7 provide illustrations of how we believe these new structures would interact to accomplish the specific national functions required for infrastructure assurance. We mean them as a guide to the types of relationships, communications, and responsibilities that might develop as the recommendations of the Commission are being implemented.

Table 3. Policy Formulation	
Assess National Risk	Support Office lead, done by contract, reviewed by Council.
Integrate Public and Private Sector Perspectives	Council lead, consultation with sectors through Sector Coordinators; Lead Agencies and special function agencies support.
Propose National Objectives and Develop Strategies	Council lead, consultation with sectors through Sector Coordinators, Lead Agencies and special function agencies; proposed to the President through the National Office.
Propose and Promote (New) Legislation	Need identified by all sources, consolidated and analyzed by Support Office, validated by National Office, drafted by Lead Agency or special function agency, reviewed by Council and OMB, submitted to Congress.
Assess and Promote (New) Regulations	Need identified by all sources, consolidated and analyzed by Support Office, validated by National Office, drafted by federal or state regulator, reviewed by Council, reviewed by normal regulatory process.
Influence Private Sector Investments	Support Office with contract support identify deficiencies (based on emerging threats) either directly with Sector Coordinators or through the Council; Council recommends to companies through Sector Coordinators.
Prepare, Recommend and Promote Budget	Council, Lead Agencies, special function agencies indicate needs and make recommendations; National Office consolidates with Support Office assistance, package reviewed by Council, Lead Agencies, special function agencies, approved by National Office, submitted to the Office of Management and Budget (OMB).
Manage and Enforce Implementation	Results reviewed by Council.
Shape the International Environment	Subset of CSG/CT prepares, annually, international objectives, meet with Department of State to fashion strategy.
Issue the National Policy	Issued by the President with an endorsement from Chair of the Council.

Table 4. Prevention and Mitigation	
Provide Effective Education and Awareness	Threat analysis provided by Information Center and training requirements identified by Sector Coordinators; consolidated by Council; vendors identified and certified by Council; other education programs coordinated by Support Office; managed by appropriate agencies, such as National Science Foundation (NSF) and Department of Education.
Set Standards, Certifications and Best Practices	Established by Sector Coordinators; forwarded to Lead Agencies if legislation or regulation is desired by companies; Lead Agencies enter into legislative or regulatory process as required, if approved by Council.
Assess Vulnerabilities and Risks of System Components	Council directs Support Office to prepare assessment instrument for each sector requesting one; Sector Coordinators review instrument; assessment vendors identified and certified by Sector Coordinators; owners and operators fund and manage.
Research Advanced Techniques; Develop New Technologies	National Office determines requirements in coordination with Lead Agencies, Council, OSTP, and private sector research organizations; Lead Agencies and/or NSF request funding and manage research as agreed.
Negotiate Funding	Owners and operators identify system upgrades based on risk assessment; Sector Coordinators propose cost share; Council serves as the forum for negotiation with Lead Agencies and representative from National Office.
Acquire the Resources for Protecting Systems	Acquired by owners and operators.
Manage Operations Consistent with Best Practices	Managed by owners and operators; performance reviewed by Sector Coordinators supported by Lead Agencies.

Table 5. Information Sharing and Operational Warning	
Share Information	Owners and operators send information on “unusual events” to Lead Agencies, as required, and to Sector Coordinator information cells (connected to intelligence and law enforcement communities); threshold events and statistics to Information Center (also connected to intelligence and law enforcement).
Analyze Information and Prepare Threat Advisories	Information Center sends general advisories to all or selected participants as needed.
Disseminate Warnings	“Actionable” warning information is relayed by teleconference to the OCIIP for decision, with copy to National Office and CSG/CT duty officer; dissemination directly to Sector Coordinators and owners and operators as per protocol.

Table 6. Counteraction (Incident Management)	
Develop Incident Management Policy and Plan Operations	FBI develops incident management policy and plans; CSG/CT reviews plans; Sector Coordinators develop plans to "close holes and block attacks" using National Office threat information and planning guidance.
Deter, Halt, or Minimize an Attack;	NSC develops deterrence policy. FBI takes lead in any attack, assesses magnitude and requests assistance as required from Defense, Intelligence or other government agencies; lead may be elevated into NSC structure, supported by National Office secretariat.
Implement Defensive Actions	FBI notifies National Office and Sector Coordinators of nature and extent of attack concurrent with standard notifications; Sector Coordinators and FBI consult on recommended provider actions; Sector Coordinators notify owners and operators.
Punish Perpetrators During or After an Attack	FBI takes lead for response to both domestic and international perpetrators unless actions have significant diplomatic implications; in which case, lead is elevated to the NSC.
Control Misinformation and Manage Perceptions	White House stands up public affairs center assisted by law enforcement and intelligence communities, DoD, National Office, and others as needed.
Coordinate Incident and Consequence Management	FBI and FEMA negotiate directly, with National Office participation.

Table 7. Response, Restoration and Reconstitution (Consequence Management)	
Plan for the Response to Consequences	FEMA leads with support of Federal Response Plan agencies and state and local emergency managers.
Manage the Response to Consequences	FEMA leads with support of Federal Response Plan agencies and state and local emergency managers.
Plan for Restoration and Reconstitution	Owners and operators plan for routine disruptions; Sector Coordinators facilitate planning with support of Lead Agencies for major disruptions; planning consolidated by FEMA.
Manage Restoration and Reconstitution	Owners and operators manage routine disruptions; Sector Coordinators work through the Federal Response Plan using Lead Agencies for major disruptions; funding to be determined under provisions of the Stafford Act (PL 93-288, as amended).

Other Federal Responsibilities

Law Enforcement

The basic law enforcement functions are not changed. There is a relatively new class of computer crimes for which classical techniques and training may not be adequate. Federal law enforcement agencies lead the country in developing new capabilities and in conducting training and awareness sessions with state and local agencies.

Intelligence Collection and Analysis

The intelligence community is expected to continue and improve its programs designed to assess the likelihood of an attack from abroad in general and to give specific warning of increasing capabilities or specific hostile intent.

Emergency Planning

Because actions needed to save lives and protect property in the event of a major disruption of infrastructure services are much the same regardless of the cause, we expect that federal emergency planning and response functions will continue as currently constituted. The real key to minimizing losses, however, will be the rapid restoration of the disrupted infrastructures. While private industry has a commendable record of restoring operations after most conventional forms of disruption, in an orchestrated attack there is a potential for damage well in excess of that normally encountered. There may, therefore, be a need to develop plans and capabilities that do not now exist. In Chapter 10, we recommend that FEMA take action to consolidate restoration and reconstitution planning and operations under the auspices of the FRP, using the designated Lead Agencies.

National Defense

Certain threats to our infrastructures may rise to the level of a national defense concern. The magnitude of the threat and required response or the identity of the attacker (from beyond our borders) may shift the lead for a cyber attack from DOJ to DoD. DoD is expected to:

1) plan counteractions to deter, halt, or minimize an attack considering a variety of possible sources and alternative responses, which may include a variety of military options;
2) coordinate selection of specific responses with the National Command Authority; and
3) execute counter-actions as authorized.

In addition, as technology enables increased detection and identification capability for cyber attacks, DoD (including its NSA component) may play an increased role in detecting potential cyber attacks before they enter the nation's domestic communications systems.

International Outreach

In the new geography, protecting our infrastructures at home is not enough. Many aspects of infrastructure operations extend beyond our national borders, and even beyond the control of

their owners and operators. The very nature of the cyber dimension renders national borders almost obsolete, and national laws and policies based on those borders of less and less consequence. Initiatives to construct partnerships between and among sectors and infrastructures must of necessity take into account the international character of business. The overall success of our own infrastructure assurance efforts will therefore require substantial international collaboration. The federal government should continue efforts to work with appropriate international bodies to address infrastructure protection concerns and raise the level of international cooperation and coordination on computer intrusion matters. An effective international regime to deter cyber crimes and cyber attacks will be more effective than purely national sanctions. Clarification of the dynamics surrounding a "cyber attack" under international law would also contribute to deterrence. Other issues worthy of international dialogue include the handling of cyber crimes that transcend borders, and legal responsibilities in multi-national infrastructures. Diplomatic efforts can also contribute to the success of our national encryption policy and the development of internationally accepted standards for computer security and information technology.

The United States is not alone in facing the realities of the new geography, but we are definitely in the vanguard of countries which have begun to realize the urgency of the issue. This gives us an opportunity to shape the contours of international cooperation in this universally important area. Just as the federal government can lead by example in the context of US infrastructure assurance, the US can help create a positive influence on the infrastructure owners and operators—as well as the governments—of the countries that reside with us in the global community.

Conclusion

Managing new risks in the Information Age requires a partnership between industry and government for many purposes, from policy making aimed at preventing a crisis through responding if such a crisis occurs. It also requires adding a cyber dimension to our existing capabilities. Our recommendations in this chapter seek to enable increased partnership with the private sector and, importantly, to increase capabilities within our existing structures (see Figure 10).

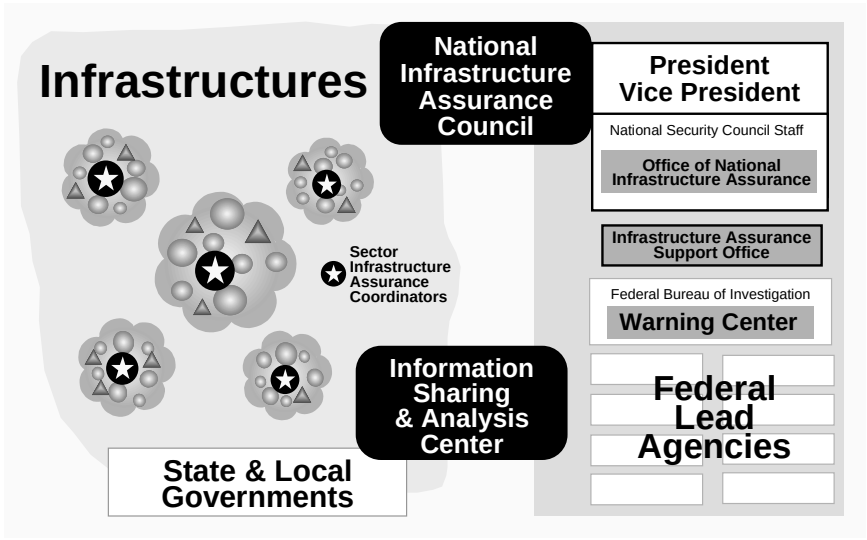

Figure 10. Proposed National Structure for Infrastructure Assurance

While we strongly endorse a policy of reliance on the private sector for problem-solving, solutions, and technology, we also see a need for a strong government focus on infrastructure protection and a federal framework to implement a national policy on infrastructure protection.

The key to success of the integrated public-private structure we propose will be "buy-in" from all sectors. And the key to their buy-in is heightened awareness of the challenges ahead. The new structures we propose are intended to generate awareness among all participants in infrastructure protection—public and private—and more broadly throughout the nation.

(Intentionally Left Blank)

Chapter Eight

Report on Awareness and Education

Objective **Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.**

The Awareness Challenge

A successful public-private partnership requires a significant level of understanding on the part of the owners and operators of the infrastructures, government, and the public at large. It is clear that one key to a more secure future is broader understanding of the role that information and telecommunications play in our national security and economic competitiveness. That understanding must be supported by an increased knowledge base throughout the nation. We must have new "street smarts" about the Information Age, about computers, and about the communications systems that connect our institutions, homes, and businesses. In short, we need a new awareness throughout the nation.

The National Research Council cited the need for greater sensitivity to information security in a 1991 report:

> *"That today's commercial (computer and software) systems provide only limited safeguards reflects limited awareness among developers, managers, and the general population of the threats, vulnerabilities, and possible safeguards. Most consumers have no real-world understanding of these concepts and cannot choose products wisely or make sound decisions about how to use them. Even when consumers do try to protect their own systems, they may be connected via networks to others with weaker safeguards — like a polluting factory in a densely populated area, one person's laxness in managing a computer system can affect many."*[12]

[12] Computers at Risk: Safe Computing in the Information Age, National Research Council, National Academy Press, Washington, DC, 1991, pp. 2-3.

There are indications that awareness of computer security issues may be increasing, as demonstrated by a recent survey of 10,000 subscribers conducted by *Info-Security News* and Deloitte & Touche. Of the 1,225 responses, 55 percent considered lack of end-user awareness to be a significant barrier to information security. This is an improvement over the 73 percent who provided a similar response two years before, but it still suggests a requirement for greater awareness of the need for special measures to ensure information security.[13]

An Awareness Program

We have some experience with awareness programs. Forty years ago, wild fires annually destroyed nearly five million acres of land in the United States. Often caused by careless hikers, these fires cost nearly $1 billion per year. The "Smokey Bear" campaign, with its "Only you can prevent forest fires" slogan, saved about $17 billion in its first 30 years.

In the infrastructure protection arena, we need to reach four target audiences: infrastructure owners and operators, corporate infrastructure users, senior governmental officials at the federal and state levels, and the general public.

We Recommend:	The White House sponsor a series of conferences with national leaders in the public and private sectors to define programs to increase the commitment to information security. White House leadership is essential to the success of an awareness program on information security.

We Recommend:	The intelligence and law enforcement communities and the proposed Office of National Infrastructure Assurance expand existing programs of communication with infrastructure owners and operators and senior governmental officials by including periodic briefings on threats and vulnerabilities, recognizing the need to comply with appropriate security considerations.

We Recommend:	The National Academy of Sciences and the National Academy of Engineering establish a Round Table bringing together federal, state, and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security and to provide continuing support to an awareness program.

[13] Info-Security News Industry Survey, May 1997, pp. 20 ff.

We Recommend:	The proposed Office of National Infrastructure Assurance, in coordination with the private sector, spearhead a continuing national awareness campaign, emphasizing infrastructure security.

We Recommend:	The proposed Office of National Infrastructure Assurance establish a program to hold infrastructure assurance simulations involving senior public and private officials. Funded from the proposed R&D budget, the simulations would assess the value of new concepts in improving infrastructure assurance. Reports on the findings of the games would be distributed as a part of the awareness campaign.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage the private sector to develop generally accepted security principles to be used by internal and external audit institutions in their regular operational audit functions in order to sustain awareness in public and private institutions.

We Recommend:	The proposed Office of National Infrastructure Assurance encourage private industry to perform periodic, quantitative risk assessments of their information and telecommunications systems, to enhance awareness of new vulnerabilities. A quantitative risk assessment addresses risk and likelihood of loss in business language and supports cost-benefit analysis for financial risk management.

An Education Program On Computer Ethics

In many families, children are more computer literate than their parents. Lacking experience, the parents seldom offer ethical guidance regarding computer usage. Universities are finding it necessary to establish new protocols for the student population in order to protect privacy and intellectual property. Computer ethics should be introduced as a field of study in all schools, from K-12 through universities.

We Recommend:	The White House convene a conference on the broad issue of computer ethics directed at the K-12 and the general university population, drawing on state and regional leaders who can support the programs in local communities, school systems, and universities.

We Recommend:	The US Department of Education commit at least $5 million per year for five years to assemble and distribute course materials and sponsor appropriate institutions for development of special programs and new course materials for K-12 and university education on the subject of the ethics of computer usage.

A Professional Education Program

There is a significant deficiency in the number of university faculty members equipped to teach information and computer security. Professor Spafford of Purdue University reports that "over the last five years, the four academic institutions teaching information security in computer science programs granted 16 Ph.D.s for security-related research. Of these, three stayed in academia."[14]

In schools of business, students majoring in information systems may learn about computer security. However, the students in other specialties who may become general managers are given little insight into the need to deal with information and communications security even in terms of their study of risk analysis.

The federal government has a number of initiatives under way in information security. DARPA has a research program that is helping in the design of security systems. NSA is developing a continuing workshop in this field. The second will be held in Austin, Texas, in 1998, organized by the University of Texas. These workshops are intended to share information about what is being taught in the field of information and communications security and how these educational programs can be extended to a larger audience.

We Recommend:	The White House convene one or more conferences of academic leaders from engineering, computer science, and business schools to review the status of undergraduate and graduate education in information security and identify changes in the curricula and the resources necessary to initiate needed changes to meet the national demand for professionals in the field.

[14] Statement of Dr. Eugene Spafford at "A Briefing on Secure Communications" before the House Committee on Science, February 11, 1997.

We Recommend:	NSF commit $10 million per year for at least five years to university programs on information assurance to support graduate students and faculty in Departments of Computer Science or in Business Schools with a view toward increasing the quality of education, the number of graduates in information and computer security, and the number of faculty members teaching in the field. As a part of such support, authorize the acquisition of advanced equipment when essential to the academic purposes of the program.

A General Education Program

Deficiencies in the training of technicians are reflected in inadequate attention to computer security in day-to-day operations. Education and training are essential to developing the staffs necessary to manage and operate major information systems today. Technicians need a deeper understanding of the systems they manage than they are likely to get if they have only on-the-job training. The rate of growth of the knowledge base makes it necessary to provide for initial training and also refresher training at regular intervals.

There are many commercial institutions in the field of education and training as well as community colleges, university extension programs, professional society programs, and others. While some have good course material, all could benefit from course material developed by the government agencies engaged in work in the field of information assurance.

We Recommend:	NIST, NSA, and the US Department of Education work in collaboration with the private sector to develop programs for education and training of information assurance specialists and for continuing education as technologies change. This effort should also support "training the trainers" to provide an adequate cadre of qualified instructors to teach technicians.

(Intentionally Left Blank)

Chapter Nine

Leading by Example

Objective **Initiate a series of information security management activities and related programs demonstrating government leadership.**

Infrastructure assurance is a joint responsibility, but the federal government has an unmistakable duty to lead the effort. Clearly, the federal government must ***lead by example*** as it reaches out to the private sector and other levels of government. We need to ensure the federal government has the policies and tools required to conduct business in the cyber age. Toward that end, the Commission makes these recommendations.

Improve Government Systems Security

The federal government has not paid sufficient attention to its own computer security needs. While OMB has developed and promulgated guidelines to ensure agencies adopt effective internal computer and network security practices, the effort to identify and replicate best practices throughout the government has fallen short of its target.

We Recommend:	Assigning systems security oversight responsibilities to the proposed Office of National Infrastructure Assurance. This will require legislative changes to restructure those responsibilities from OMB to the new office.

We Recommend:	The Secretary of Commerce and the Secretary of Defense charge NIST and NSA with assisting federal agencies in the implementation of best practices for information security within their individual areas. The process should include a NIST/NSA-facilitated assessment of agency vulnerabilities and security practices with input from the proposed Office of National Infrastructure Assurance.

We Recommend:	The FBI actively recruit college students with appropriate computer-related technical skills to seek employment with the Bureau. The FBI should consider offering part-time employment for skilled college students with regional computer crime squads. This program could produce current benefits as well as future special agent and forensic examiner applicants qualified to investigate cyber crime matters.

We Recommend:	The FBI facilitate hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks. Three years of service in cyber-related activities could be a condition of employment for those who receive a hiring preference based on computer skills.

Encryption

For electronic commerce to flourish, the information infrastructure must be secure and reliable. Protection of the information our critical infrastructures are increasingly dependent upon is in the national interest and essential to their evolution and full use. A secure information infrastructure requires the following:

- Secure and reliable telecommunications networks.
- Effective means for protecting the information systems attached to those networks.
- Effective means for authenticating communications of trading partners, assuring the integrity of data and non-repudiation of transactions.
- Effective means of protecting data against unauthorized use or disclosure.
- Well-trained users who understand how to protect their systems and data.

Strong encryption is an essential element for the security of the information on which critical infrastructures depend. Establishment of trustworthy key management infrastructures (KMIs) is the only way to enable encryption on a large scale, and must include the development of appropriate standards for interoperability on a global scale. Key recovery is needed to provide business access to data when encryption keys are lost or maliciously misplaced, and court-authorized law enforcement access to the plain text of criminal-related communications and data lawfully seized.

Neither private citizens nor businesses are likely to use the information infrastructure on a routine basis if they lack confidence that their communications and data are safe from modifica-

tion or unauthorized access. To ensure public confidence in key recovery, stored decryption keys must receive the same sort of legal protections that currently exist for mail, telephone communications, and electronic communications, including e-mail. To fairly balance the competing equities of privacy, electronic commerce, national security and law enforcement, and to ensure public confidence, the following are necessary:

- The public should be free to select an agent to issue digital signatures or to serve as a key recovery agent.
- Law enforcement agencies should have lawful access to the decrypted information when necessary to prevent or detect serious crime. Procedures for judicial review prior to granting government access must be defined in law.
- Individual rights of redress when access is abused should also be defined in law.

We Recommend:	Expediting the several government pilot projects underway or recently announced as a means of testing the technical and policy concepts involved and building public confidence and trust with the KMI key recovery approach. Further, the Administration should promote efforts to plan for the implementation of a KMI that supports lawful key recovery on an international basis. Finally, the federal government should encourage efforts by commercial vendors to develop key recovery concepts and techniques.

Procurement

We Recommend:	An interagency task force identify large pending procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance issues, study whether infrastructure assurance objectives are being considered, determine how they may be adapted, and, based on the lessons learned, propose revisions to the overall procurement process.

Threat Assessments

We Recommend:	The federal government elevate and formalize information threats as a foreign intelligence priority.

NIST Risk Assessment

We Recommend:	NIST and appropriate government agencies continue development of risk assessment methodologies and make these known and available to the private sector, especially owners and operators of infrastructures.

Measuring Performance

The Government Performance and Results Act (GPRA) requires five-year strategic plans and performance measures for major functions and operations of federal agencies to be reviewed by OMB in the budget process. The Information Technology Management Reform Act (ITMRA) requires performance measures related to the use of information technology. The required performance measures do not, however, specifically include information security.

We Recommend:	The Administration direct federal agencies to include assigned infrastructure assurance functions within their GPRA strategic planning and performance measurement framework.

We Recommend:	The Administration and Congress amend the ITMRA to require that agency Chief Information Officers develop performance measures for the security of their information systems and to submit evaluations to OMB as required by the statute.

Certification Programs

The Environmental Protection Agency (EPA), NSA, and others have demonstrated ways of extending the benefits of federal standards or certifications to the private sector. The Commission noted the EPA's ENERGY STAR program as an example of such an effort. A recently-initiated certification partnership between NSA, NIST, and industry is designed to facilitate the evaluation of commercial information assurance products. These low cost, easily administered mechanisms encourage voluntary compliance with federal standards.

We Recommend:	Lead Agencies consider the creation and use of certification programs that are inexpensive to administer and enforce, and that provide incentives for adoption of standards for information security and information technology services and products.

Global Positioning System

The GPS is scheduled to be the sole source of radionavigation for aircraft landing guidance systems by the year 2010. Although cost-efficient, this creates the potential for single-point failure.

We Recommend:	The Secretary of Transportation: • Fully evaluate actual and potential sources of interference to, and vulnerabilities of, GPS before a final decision is reached to eliminate other radionavigation and aircraft landing guidance systems. • Sponsor an independent, integrated assessment of risks to civilian users of GPS-based systems, projected through the year 2010. • Base decisions regarding the proper federal navigation systems mix and the final architecture of the modernized NAS on the results of that assessment.

National Airspace System

The proposed architecture for the modernized NAS appears to have vulnerabilities that should be given full consideration before the final design is approved.

We Recommend:	The Federal Aviation Administration (FAA) act immediately to develop, establish, fund, and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions, intrusions and attack. Program implementation should be guided by the recommendations found in the *Vulnerability Assessment of the FAA National Airspace System Architecture*, prepared for the Commission.

(Intentionally Left Blank)

Chapter Ten

Legal Initiatives

Objective **Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.**

Infrastructure protection requires the integrated capabilities of diverse federal agencies, and special means for coordinating federal response to ensure that these capabilities are melded effectively together. The first step in defining federal structures to support infrastructure assurance in the Information Age must be to understand how responsibility is assigned today within the legal framework of the federal government.

The interdependence of all the infrastructures and the critical role of the information and communications infrastructure in all aspects of American life create special jurisdictional challenges. These jurisdictional problems are further complicated by the continued growth in cyber attack capabilities across the threat spectrum. The ability to know the origin, purpose and magnitude of an attack is significantly limited today. Consequently, we do not have the sharp and unambiguous jurisdictional cues that guide decisions about response and assignments of responsibility in the more familiar physical arena. We may not know the source of an attack—domestic or foreign. We may not know the identity or motives of the attacker—individual or group, terrorist, criminal, or government. Nor may we know the magnitude of the attack—whether a single system is involved or the attack is perpetuated throughout a network or series of networks. We may not even know if ours is the only nation experiencing the attack.

Given the lack of knowledge available at the initiation of an attack, it is clear that any required federal response will be borne on the Attorney General's authority as the nation's chief law enforcement officer. Elements of the response may require support of the defense, emergency response, intelligence and diplomatic agencies, as well as other agencies within government. There is a clear need to have required decision support, planning capabilities, and response authorities available to the Attorney General and to the White House should the decision reach that level.

The structures we recommend in Chapter 7 recognize that infrastructure assurance is more than a law enforcement, defense, or economic problem. It encompasses the responsibilities of each of

these areas, and also of the owners and operators who actually deliver infrastructure services. The federal government must not only integrate the familiar elements of government; it must also lead an effort to enhance the protection capabilities inherent in the infrastructures themselves, and generate the kind of trusted environment that enables a cohesive public-private partnership to accomplish all the functions involved in infrastructure protection.

We recognize also that while responsibilities are widely shared within the government, the current level of technology does not allow the posture of deterrence and forward defense that protects us from foreign military and terrorist threats in the physical dimension. Initially, all cyber attacks will have to be treated as crimes—regardless of where they originated or the purpose of the attack. When investigation provides evidence of foreign government involvement or the magnitude of the attack requires it, other leadership may be assigned. This also will require that the Attorney General have available immediate support from defense, intelligence and elsewhere in the government—especially from those agencies that have special skills and knowledge applicable to the cyber arena.

In making recommendations about increased partnership and better two-way sharing of information, we do not mean to indicate lack of support for existing efforts to build required information centers, watch centers, and command and control facilities. These efforts to enable response to cyber threats—criminal, terrorist or other—must continue. The organizations detailed in our recommendations are designed to expand the reach of existing capabilities, provide a means to coordinate and integrate them with information, knowledge and skills from the infrastructure owners and operators, and generally facilitate their efforts.

In addition to examining these jurisdictional issues, the Commission studied the legal foundations for infrastructure protection, and focused on the need to revisit the current law in light of infrastructure assurance objectives. In so doing, the Commission was able to make recommendations designed to enable the federal government to take a leading role, the private sector to respond, and the government and the private sector to engage in an effective partnership. Some of these recommendations, such as those relating to government model performance and legal impediments to information sharing, are highlighted in other parts of this report. Those recommendations as well as those contained in this chapter will provide a legal foundation for cultural change.

Enabling the Federal Government to Take the Lead

The first set of recommendations revisits existing legal frameworks for federal response to and deterrence of incidents involving the critical infrastructures.

Many areas of federal legislation that enable prevention and mitigation, response, recovery and reconstitution to incidents involving the critical infrastructures were written before the emergence of a recognizable cyber threat. It is not clear whether many of these authorities would apply, or should apply, to a major cyber-related event. Until the dynamics of such an event are better understood, major legislative change is premature. However, the Commission was able to identify key issues and make general recommendations to incorporate infrastructure assurance considerations within these legislative frameworks.

Defense Production Act

The Defense Production Act (DPA) provides authority to assist the reconstitution of critical infrastructures. The Commission reviewed DPA authorities, triggering mechanisms, and current modernization efforts for application to emerging threats, vulnerabilities, and related challenges.

We Recommend:	The Administration and Congress review the DPA in light of infrastructure assurance objectives. Specifically, we suggest: • Congress consider amending the DPA Declaration of Policy to include a finding that critical infrastructures are essential to national security. • Lead agencies associated with the critical infrastructures study the energy provision for priorities in contracts as a potential model for reconstituting other critical infrastructures. • Congress continue funding for the DPA Fund and financial incentives, and make funds available for R&D related to the critical infrastructures. • The Administration direct federal agencies with authorities pertaining to the critical infrastructures to review DPA authorities and work with industry to use these authorities when needed in response to a critical infrastructure incident.

Stafford Act/Federal Response Plan

The Stafford Act and FRP set parameters for federal response to major disasters as declared by the President. FEMA's authority to prepare for, mitigate, and respond to incidents affecting the operation of the critical infrastructures is unclear under the triggering mechanism currently contained in the statute.

Current FRP capabilities are responsive to infrastructure disruption. The capabilities and expertise to restore and reconstitute the infrastructures reside almost exclusively in the private sector and the main burden for planning and operations falls on the owners and operators of the infrastructure companies themselves.

However, the federal government has a shared responsibility to ensure that these infrastructures are restored rapidly in the event of a major disruption. The federal government should share in the costs of training and exercising, and ensure the availability of critical resources on a yet to be determined cost-sharing basis.

We Recommend:	The proposed Office of National Infrastructure Assurance study the Stafford Act, other authorities, and Federal Response Plan mechanisms for suitability in cyber-induced disasters. The study should address the potential impact of infrastructure failures and the desirability of direct assistance to infrastructure owners and operators.

We Recommend:	FEMA consolidate restoration and reconstitution planning and operations under the auspices of the Federal Response Plan, using the designated Lead Agencies.

Nunn-Lugar-Domenici

The Nunn-Lugar-Domenici legislation focused federal resources on providing training, access to equipment, and information to local first responders. State and local police, fire, and medical officials are requesting an expanded effort in this area. The Commission sees the need for more resources for training and equipment, and possibly an expanded scope to address other infrastructure-related events.

We Recommend:	Congress consider expanding the current Nunn-Lugar-Domenici program to incorporate other critical infrastructure issues, including attacks on infrastructures by means other than weapons of mass destruction, as well as training and information sharing efforts directed at state and local responders.

Adequacy of Criminal Law and Procedure for Infrastructure Assurance — Physical

In addition to the preventive aspects of the DPA, Stafford Act, and Nunn-Lugar-Domenici legislation, deterrence also plays an important preventive role against attacks on critical infrastructures. Deterrence through criminal law should be built not only through federal investigative and prosecutive capabilities, but also state, local, and international response.

Sentencing Guidelines

The Commission concluded there is adequate "legal fortification" from physical attacks. However, we identified several shortfalls relating to deterrence of crimes against critical infrastructures. The Sentencing Guidelines do not adequately address the severity of consequential damages arising from attacks on critical infrastructures—for example, damage resulting from the "downstream" effects of a denial-of-service attack. Consequently, a possibility exists of disproportionately light sentences for some forms of attack on critical infrastructures.

We Recommend:	The US Sentencing Commission expand the Guidelines to include greater flexibility to address actual and consequential damages, including "downstream" damage to property or loss of service resulting from attacks on critical infrastructures.

We Recommend:	The Sentencing Commission consider expanding coverage of its Guidelines to better address consequences of the use of biological and chemical weapons not resulting in death.

Interstate Commerce

The Commission identified two potential deficiencies with respect to purely intrastate attacks against critical infrastructures—even when attacks result in severe damage. In these instances, in order to assume jurisdiction over an investigation or prosecution, the federal government must demonstrate on a case-by-case basis that the incident affects interstate commerce. This is a difficult determination to make at the earliest stages of an investigation, before the scope of an attack is known or its effects are contained.

We Recommend:	Congress consider defining certain critical infrastructures as "instrumentalities of interstate commerce" to enable immediate investigation by federal law enforcement agencies and to subject those convicted to stiffer federal penalties.

Reward/Payment for Information Programs

The Commission reviewed legislation that offers rewards for information leading to the capture of terrorists. Under these legal authorities, Congress authorizes the Attorney General and the Secretary of State to administer rewards and payment-for-information programs. These laws effectively supplement other federal crime legislation to protect critical infrastructures.

We Recommend:	The monetary reward programs for information leading to capture and arrest of criminals be included as a line-item in participating federal agencies' budgets to ensure proper funding and implementation.

Adequacy of Criminal Law and Procedure for Infrastructure Assurance — Cyber

State & Local

Efforts are ongoing in most states to draft effective computer crime legislation. Dealing with juvenile computer crime is an area requiring greater attention. The states and federal government may be able to learn from innovative efforts in this area and consider modification to their laws to address what may be a growing problem.

We Recommend:	DOJ sponsor a comprehensive study aimed at compiling demographics of computer crime, comparing various state approaches to computer crime and discovering effective ways of deterring and responding to computer crime and abuse by juveniles.

Federal

The US Sentencing Commission's revised guidelines for the Computer Fraud and Abuse Act expanded definitions of "harm" and "loss" to include interruptions in service; disruptions or delays in delivery of vital services endangering lives; invasions of privacy; and the cost to the victim of damage assessment, restoration of service and data, and loss of business revenue due to interruption of service.

We Recommend:	The Sentencing Commission consider expanding its broader reformulation of harm and loss (in Guidelines Section 2B1.1, as it applies to violations of the Computer Fraud and Abuse Act and theft of trade secrets) to other forms of electronic crime and crimes relating to information and information technology.

DOJ is currently exploring ways to ease administrative burdens on federal law enforcement officers investigating various forms of computer and high technology crimes that cross federal jurisdictional boundaries. Of specific concern is allowing electronic searches to be conducted across jurisdictional boundaries with the authorization of only one federal judge.

We Recommend:	The Administration endorse and promote efforts currently underway to develop procedural changes to assist law enforcement in the investigation of computer crime, including modification of existing procedures for an effective nationwide trace and search warrant capability. Congress consider expeditious enactment of such legislation.

International

The US is a leader of efforts to clarify and improve current law enforcement procedures pertaining to computer crime.

We Recommend:	The Administration lead efforts to clarify and improve current procedures for investigating computer crime; work to create a network of international law enforcement agencies and telecommunications carriers to facilitate international investigations of computer crimes; and continue efforts to enhance international cooperation in computer crime investigations.

Legal Impediments to Vulnerability Assessments

Existing laws may create unnecessary legal impediments to the performance of vulnerability assessments on federal computer systems. The Computer Fraud and Abuse Act criminalizes a wide variety of misconduct premised on unauthorized access to government (and private) computer systems. The legislation is silent, however, as to how Red Teams might be *authorized* to attempt penetrations without running afoul of the criminal law. Legislative change does not appear to be required, but agencies should clarify procedures to facilitate sound vulnerability assessment practices.

We Recommend:	Federal agency Chief Information Officers establish procedures for obtaining expedient and valid authorization to allow vulnerability assessments to be performed on government computer systems. This requires a clear designation by agencies regarding who may authorize access to their computer systems for this purpose.

Enabling Private Sector Response

In addition to reviewing federal authorities that could be strengthened or expanded to allow the federal government to more adequately accomplish infrastructure assurance objectives, the Commission also considered potential legal impediments that might prevent owners and operators from taking appropriate action to safeguard portions of critical infrastructure within their control and responsibility. The recommendations contained in this section focus on providing owners and operators greater ability to take protective action.

Private Intrusion Response

Unauthorized intrusions often go undetected; when detected they may not be reported. Currently, computer security specialists and even state-licensed private investigators are gearing up to support private sector needs for computer security services. While their services fulfill some

victims' needs for confidentiality and control, potentially valuable information that could be used to assess the scope and nature of the threat is lost. Furthermore, there are no mechanisms in place to ensure the professionalism, qualifications, and methods by which these private investigations are performed.

We Recommend:	Congress consider new ways of facilitating the growth of private sector cyber-security capabilities that encourage increased sharing of information relevant to the scope and nature of the threat.

One approach to this area is nationwide licensing of private security specialists by a professional organization or the government. It might be possible to arrive at a professional licensing scheme that would provide benefits to a number of parties by specifying, for example, qualifications for obtaining a license, levels of insurance required, standards of practice, and conditions to allow for limited information sharing.

Additional prosecutive capabilities may also contribute to the current level of deterrence for computer-related violations. Prosecutive capabilities could be expanded by permitting victims the right to proceed in private civil actions. Civil remedies are currently available at federal and state levels. Improving the international availability of civil remedies is a logical extension of these efforts.

We Recommend:	The President seek to expand the availability of civil remedies for computer-related violations through appropriate multilateral and bilateral agreements.

Privacy Legislation and the Employer-Employee Relationship

"Insiders" provide the most frequent avenue of attack to the nation's critical infrastructures. The federal government guards against insiders' misdeeds through authority to conduct background investigations and periodic reinvestigations. Private employers who operate some of the critical infrastructures do not have the same ability. In many states, private employers do not have access to criminal history information; are prohibited from requesting or using criminal, financial or employment information; and may incur tort liability for revealing unfavorable employment history. These restrictions result from legitimate concerns over privacy, fair employment, rehabilitation, and related questions. We believe security considerations justify limited exemptions from these restrictions.

We Recommend:	The Attorney General convene a group of professionals from law, state and federal legislatures, labor and management organizations, and the privacy community to explore existing laws and recommend measures to balance employers' needs against individual interests in privacy.

We Recommend:	State legislatures consider adopting "consent" as a baseline for allowing employers to request background information from employees and potential employees for sensitive positions within critical infrastructures, subject to fair information practices.

We Recommend:	Congress narrowly expand existing exemptions to the Employee Polygraph Protection Act to include providers of information security services within the scope of its exemptions. This would update the legislation that currently allows polygraphs only to physical security services for certain public services.

Chapter Eleven

Research and Development

Objective

Increase investment in infrastructure assurance R&D from $250 million to $500 million in FY 99, with incremental increases in investment over a five-year period to $1 billion in FY 04. Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.

Federal R&D efforts are inadequate for the size of the R&D challenge presented by emerging cyber threats. Only about $250 million per year is being spent on federal infrastructure assurance-related R&D, of which 60 percent—$150 million—is dedicated to information security. There is very little research supporting a national cyber defense. The Commission believes that real-time detection, identification, and response tools are urgently needed. We concluded that market demand is currently insufficient to meet these needs.

R&D for infrastructure protection requires partnership among government, industry, and academia to ensure a successful and focused research and technology development effort.

We Recommend:	The President propose an increase in the federal investment in infrastructure assurance research to $500 million in FY99 and incremental increases in annual funding over a five-year period to $1 billion in FY04 for a targeted R&D program focusing on the six R&D areas listed below. • ***R&D Increases for Information Assurance***. Assurance of vital information is increasingly a key component to the functioning of our interdependent infrastructures. The urgent need to develop new, affordable means of protection is apparent, given the increasing rate of incidents, the expanding list of known vulnerabilities, and the inadequate set of solutions available. • ***R&D Increases for Intrusion Monitoring and Detection.*** Reliable automated monitoring and detection systems, timely and effective information collection technologies, and efficient data reduction and analysis tools are needed to identify and characterize structured attacks against infrastructure.

	• ***R&D Increases for Vulnerability Assessment and Systems Analysis***. Advanced methods and tools for vulnerability assessment and systems analysis are needed to identify critical nodes within infrastructures, examine interdependencies, and help understand the behavior of these complex systems. Modeling and simulation tools and test beds for studying infrastructure-related problems are essential for understanding the interdependent infrastructures. • ***R&D Increases for Risk Management Decision Support***. Decision support system methodologies and tools are needed to help government and private sector decision-makers effectively prioritize the use of finite resources to reduce risk. • ***R&D Increases for Protection and Mitigation***. Real-time system control, infrastructure hardening, and containment and isolation technologies are needed to protect infrastructure systems against the entire threat spectrum. • ***R&D Increases for Incident Response and Recovery***. A wide range of new technologies and tools are needed for effective planning, response, and recovery from physical and cyber incidents that affect critical infrastructures.

We Recommend:	The National Research Council define, more fully, a national infrastructure assurance research program and lead an effort with departments and agencies already engaged in R&D relevant to each infrastructure.

Assuring Water Quality

Few infrastructures are taken for granted more than our fresh water systems. There is little chance of a threat reducing the quantity of available water sufficiently to endanger the population or cause industrial collapse. But there is risk of malicious attacks over time undermining public confidence. Alternatives for protecting the water supply are few. The most feasible approach we found is a research effort focused on water contamination detection technologies. Effective applications could be developed commercially and implemented at the state and local level.

We Recommend:	The creation of a specific R&D program to provide the scientific knowledge and technology necessary to allow highly toxic chemical and biological agents to be detected, identified, measured and treated in near real-time in the nation's water supply systems. The program should be administered by the EPA.

Provide Early Warning and Response

Real time detection of cyber threats is a special challenge to the R&D community. While this area is included in our recommendation above for additional R&D investment, it is central to the future security of our infrastructures. Some effort is under way, but it requires continued funding and high priority.

Although many industry and government groups are dedicated to ensuring the technical performance of next generation telecommunications networks, there has been no cohesive effort for protecting this infrastructure against the emerging threat of cyber attack. Such effort should include a system of surveillance, assessment, early warning, and response mechanisms to mitigate the potential for cyber threats. Although current methodology for this centralized effort does not exist, several of the basic technical elements required are successfully deployed on a small-scale basis, or in research, and could be integrated into a limited cohesive, national cyber response element.

Conceptually, a successful cyber attack warning and response system would include:

1) A means for near real-time monitoring of the telecommunications infrastructure.
2) The ability to recognize, collect, and profile system anomalies associated with attacks.
3) The capability to trace, re-route, and isolate electronic signals that are determined to be associated with an attack.

We Recommend:	The R&D program include a priority effort to develop such an Early Warning and Response capability.

Chemical and Biological Agent Detectors

Considering the serious and growing threat of a chemical or biological attack, chemical and biological agent detectors and effective protective and clean-up equipment are urgently needed and should be included in R&D efforts.

(Intentionally Left Blank)

Chapter Twelve

Implementation Strategy

This strategy provides the framework of objectives which will establish the foundations for a longer-term effort to assure our critical infrastructures. It describes major actions leading to fulfillment of each objective, and the expected outcome over the three-year period following a decision by the President to implement the Commission's recommendations. A more detailed implementation plan, with time lines, will be provided during the interagency review of the Commission's recommendations.

Strategic Objectives

Objective 1

Promote a partnership between government and infrastructure owners and operators beginning with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

Anticipated Three-Year Outcome

An active program which exchanges information on anomalous activities and suspicious incidents and distributes meaningful integrated analyses of government and private sector data, and threat and warning information, on an almost real-time basis to appropriate decision-makers in both government and private industry.

Action Items

- Develop a planning framework for establishing an Information Sharing and Analysis Center, jointly staffed by government employees and representatives from the critical infrastructures, to receive information from all relevant sources and conduct analyses for dissemination to participants.

- Designate selected federal departments and agencies to assume Lead Agency responsibilities.

- Coordinate with DOJ, other federal agencies, and the private sector to resolve legal impediments to information sharing, including potential antitrust, tort liability, national security, classification, disclosure, and protection of proprietary and trade secret information issues.

- Assist infrastructure stakeholder selection of Sector Infrastructure Assurance Coordinators to facilitate sharing of information among critical infrastructure owners and operators and with the government.

- Develop interagency infrastructure information sharing guidelines.

- Initiate personnel hiring process, identify an appropriate site, and stand up the Information Sharing and Analysis Center.

Objective 2

Ensure infrastructure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles.

Anticipated Three-Year Outcome

Infrastructure owners and operators able to make better informed assurance investment decisions; local and state governments better equipped and trained to protect critical infrastructures and respond to untoward events.

Action Items

- Facilitate the efforts of NSA, DOE, and DoD to provide private sector assessments for critical infrastructure owners and operators; facilitate the offer of additional, more encompassing assessments over a range of cyber, physical, and interdependency risks; and provide vulnerability assessment training to private sector service providers on a cost-reimbursable basis.

- Encourage the private sector to develop generally accepted security principles to be used by internal and external audit institutions in their regular operational audit functions.

- Convene a group of professionals from law, state and federal legislatures, labor and management organizations, and the privacy community to examine existing laws in light of infrastructure assurance objectives and recommend measures to balance the legitimate needs of critical infrastructure owners and operators to conduct appropriate employee background investigations with the privacy rights of individual employees.

- Coordinate the continued development of risk assessment technologies, and associated tools, policies, procedures, and practices with appropriate federal agencies; encourage the transfer of these methodologies to the private sector; and encourage private sector performance of periodic quantitative risk assessments.

- Coordinate the development of mechanisms for disseminating information about infrastructure assurance to state and local governments.

- Encourage state legislatures to consider adopting "consent" as a baseline for allowing employers to request background information from employees and potential employees for sensitive positions within critical infrastructures, subject to fair information practices.

- Sponsor federal legislation to narrowly expand existing exemptions to the Employee Polygraph Protection Act to include providers of information security services within the scope of its exemptions.

Objective 3

Establish national structures that will facilitate effective partnership between the federal government, state and local governments, and infrastructure owners and operators to accomplish national infrastructure assurance policy, planning, and programs.

Anticipated Three-Year Outcome

A formal structure that encourages private industry participation in development of a national policy for infrastructure assurance, identifies the capabilities and responsibilities of federal agencies for infrastructure continuity, and facilitates national incident planning, response, mitigation, and restoration activities.

Action Items

- Establish an interagency working group to develop a plan for stand-up of structures that will contribute to the development of a national infrastructure assurance policy, including an Office of National Infrastructure Assurance; a National Infrastructure Assurance Council; an Infrastructure Assurance Support Office; and a Lead Agency to act as the government's focal point for each of the various infrastructure sectors.

- Review the FRP and other applicable documents to assist the FEMA's consolidation of restoration and reconstitution planning relating to cyber infrastructure assurance issues.

- Review results of legislative initiatives and other studies articulating roles and responsibilities of federal agencies for assurance issues; coordinate issues with appropriate entities.

- Coordinate a National Infrastructure Assurance Policy through government and private sector representatives.

Objective 4

Elevate national awareness of infrastructure threat, vulnerability, and interdependency assurance issues through education and other appropriate programs.

Anticipated Three-Year Outcome

A more informed private industry, government and general public who understand critical infrastructures; individuals and institutions who understand the need to protect their own use of information as well as information used by others; general appreciation of the need to develop a broader base of information assurance technical talent; and sharper focus on computer ethics and advanced information security technology in education programs.

Action Items

- Sponsor a series of White House conferences with academic and industry leaders from the public and private sectors to reach consensus on a plan of action that will increase the commitment to information security; emphasize computer ethics for grades K-12 and the general university population; review the status of undergraduate and graduate education relating to infrastructure protection, particularly information security; and define continuing opportunities to meet the national demand for professionals in the field.

- Coordinate with the National Academy of Sciences and the National Academy of Engineering to establish a Round Table in parallel with those in other fields, bringing together federal, state, and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure assurance.

- Obtain NSF funding to support programs of professional education in university computer science departments and business schools.

- Coordinate with intelligence, law enforcement and regulatory agencies to expand programs for CEO briefings relating to infrastructure threats and vulnerabilities.

- Sponsor a feasibility study of publishing comparative infrastructure assurance-related data for certain infrastructures.

- Lead a public service campaign, in coordination with the private sector, to emphasize awareness of the threats and vulnerabilities of infrastructures and methods of improving infrastructure security.

Objective 5

Initiate a series of information security management activities and related programs demonstrating government leadership.

Anticipated Three-Year Outcome

Federal government information and networks are better protected from unauthorized intrusion, disruption, or modification using management procedures recognized as “best practices” and transferable to private industry.

Action Items

- Select a lead agency for assisting federal entities in the implementation of best practices for information security.
- Assign responsibilities for federal computer network security to the proposed Office of National Infrastructure Assurance.
- Encourage law enforcement to initiate new programs to hire and retain qualified personnel for investigative and analytical positions involving cyber issues.
- Fully evaluate threats and vulnerabilities associated with deployment of the GPS prior to elimination of other radionavigation and aircraft landing guidance systems.
- Develop, establish, fund, and implement a comprehensive security program to protect the modernized NAS from information-based and other disruptions, intrusions and attack.
- Resolve issues associated with spectrum allocation for communications among and between emergency service providers.
- Prepare an Executive Order requiring federal agencies to weigh the positive and negative effects on inrastructure assurance before publishing or requiring publication of information about critical components or functioning of infrastructures.
- Facilitate infrastructure assurance simulations within the federal government, and disseminate findings as part of the awareness campaign.

Objective 6

Sponsor legislation to increase the effectiveness of federal infrastructure assurance and protection efforts.

Anticipated Three-Year Outcome

Updated legislation that addresses critical infrastructure issues and enhances law enforcement ability to successfully investigate and prosecute related criminal activities.

Action Items

- Sponsor an interagency task force or other review mechanism to determine applicability of delineating infrastructure assurance objectives in the Information Technology procurement process; the Government Performance and Review Act; the Information Technology Management Reform Act; the Stafford Act; Nunn-Lugar-Domenici; and, the FRP.

- Formalize information threats as a foreign intelligence priority.

- Sponsor legislative activities leading to a finding that certain critical infrastructures are "instrumentalities of interstate commerce."

- Promote broader agency use of programs that provide monetary rewards for information relating to infrastructure attacks.

- Review information required by law to be published to ensure vulnerabilities are not disclosed.

- Coordinate DOJ sponsorship of a study to compile demographics of computer crime offenders, including juvenile offenders.

- Encourage the US Sentencing Commission to consider expanding its broader reformulation of harm and loss (in Guidelines Section 2B1.1, as it applies to violations of the Computer Fraud and Abuse Act and theft of trade secrets) to other forms of electronic crime and crimes relating to information and information technology.

- Endorse efforts currently underway to develop an effective nationwide trace and search warrant capability; and efforts to facilitate international cooperation in computer crime matters.

- Encourage the Sentencing Commission to expand guidelines to include greater flexibility to address actual and consequential damages, including "downstream" damage to property or loss of service resulting from attacks on critical infrastructures and, to better address consequences of the use of biological and chemical weapons not resulting in death.

Objective 7

Increase investment in infrastructure assurance research from $250 million to $500 million in FY99, with incremental increases in investment over a five-year period to $1 billion in FY04.

Target investment in specific areas with high potential to produce needed improvements in infrastructure assurance.

Anticipated Three Year Outcome

A focused and accelerated program which delivers usable tools to fill gaps in technology in infrastructure assurance.

Action Items

- Facilitate the establishment of a national focal point for infrastructure assurance R&D efforts and a public/private/academic sector partnership to foster technology advancement and transfer.

- Develop a comprehensive plan to focus R&D on technical solutions to infrastructure assurance issues associated with information security management, intrusion detection, vulnerability assessment and systems analysis, risk management and decision support, protection and mitigation, and incident response and recovery.

- Initiate an R&D program in cooperation with the water system owners and operators to identify vulnerabilities of water supply systems and to evaluate mitigation techniques.

(Intentionally Left Blank)

O n w a r d

Originally, we had intended to title this final section of the report as a conclusion. It is anything but conclusion. In fact, it is a beginning. Our entire effort is prologue to a new era of infrastructure assurance.

This is not an exercise in problem solving. It is an attempt to deal with a rapidly changing, technology driven environment in which information and communications technologies add a new dimension of concern. In effect, we are not proposing solutions, but offering a step toward posturing our nation more effectively to deal with a new, still evolving world.

Our nation is in the midst of a tremendous cultural change, which will have a profound effect on our institutions. Accordingly, we are offering first steps toward preparing our critical infrastructures—and our government—to deal with this change. We believe that the only way to assure the future security of the nation is by assuring our critical infrastructures. And doing that will require a vigorous, innovative partnership between our government and the owners and operators of those infrastructures.

We offer these recommendations with a sense of urgency. While we do not believe a debilitating attack is imminent, the threats to our nation and the vulnerabilities in our infrastructures are real.

And the time to act is *now* . . .

(Intentionally Left Blank)